Universidad Carlos III de Madrid

Departamento de Ingeniería Mecánica

PROYECTO FIN DE CARRERA

PROCEDIMIENTO PARA LA GENERACIÓN DE UN DOSSIER DE SEGURIDAD PARA LA IMPLEMENTACIÓN DEL SISTEMA DE SEÑALIZACIÓN FERROVIARIA ERTMS NIVEL 1 EN UNA APLICACIÓN ESPECÍFICA

Autor: D. Álvaro Nebrera Porras

Tutor: D. Ricardo del Río Rubio

Leganés, Septiembre de 2015

Título: Procedimiento para la generación de un Dossier de seguridad para la implementación del sistema de señalización ferroviaria ERTMS Nivel 1 en una aplicación específica.
Autor: D. Álvaro Nebrera Porras
Director: D. Ricardo del Río Rubio

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Agradezco a mis padres por habérmelo dado todo para llegar hasta aquí, por los valores que me han transmitido y la educación que he podido disfrutar gracias a ellos. A mis hermanos por ayudarme siempre que lo he necesitado, y a Mariló, por creer siempre en mí y por animarme a ir siempre un poco más allá.

Resumen

El objeto del presente proyecto es el de describir de una manera sencilla el proceso que es necesario llevar a cabo con el fin de generar un Dossier de Seguridad que permita la implementación del sistema de señalización ferroviaria ERTMS (*European Railway Traffic Managment System*) Nivel 1 en una aplicación específica.

Cuando se habla de Dossier de seguridad se hace referencia al conjunto de documentación (planes, pruebas, informes, etc.) que es necesario elaborar para cumplir con las especificaciones dictadas por la norma CENELEC EN-50126.

Dicha norma (CENELEC EN 50126) especifica el ciclo de vida que hay que completar para poder implementar con seguridad un sistema de señalización ferroviario en una aplicación específica determinada. Este ciclo de vida consta de una serie de fases que se irán detallando a lo largo del presente proyecto.

Con el fin de ampliar el conocimiento sobre el sistema de señalización ERTMS N1, en primer lugar se va a describir de manera resumida su funcionalidad y los elementos que lo componen.

Por último se irán definiendo cada una de las distintas fases que forman el ciclo de vida descritas en la norma; y dentro de cada fase se irán determinando las actividades y documentos que el Ingeniero de Seguridad o el equipo de Seguridad deben realizar.

Palabras clave: Dossier de Seguridad, RAMS, ERTMS Nivel 1, Norma CENELEC EN-50126, Fases del ciclo de vida, Amenazas, Riesgos, Medidas de mitigación.

Abstract

The purpose of this project is to describe in a simple way the process that is necessary to carry out in order to generate a Security Dossier that enables the implementation of the rail signaling system ERTMS (European Railway Traffic Management System) Level 1 in a specific application.

The safety dossier is referred to the set of documents (plans, test reports, etc.) that need to be developed to meet specifications dictated by the standard CENELEC EN-50126.

This standard (CENELEC EN 50126) specifies the life cycle to be completed in order to implement with safety a rail signaling system in a given specific application. This life cycle consists of a series of phases that will be specified throughout this project.

In order to increase knowledge about the signaling system ERTMS N1, first of all it will be described its functionality and the elements that compose it.

Finally it will be defined each one of the various phases forming the life cycle described in the standard; and within each phase it will be determined the activities and documents the Safety Engineer or Safety team must perform.

Keywords: Safety Dossier, RAMS, ERTMS Level 1, CENELEC EN-50126 Standard, Life cicle phases, Threats, Risk, Mitigation measures.

Índice general

Índice de figuras

Índice de tablas

1.Introducción y objetivos

1.1 Introducción

En los últimos años, los medios de transporte han evolucionado a una gran velocidad. Y posiblemente, el ferrocarril haya sido el que más lo haya hecho. Multitud de kilómetros de vías férreas se han construido, consiguiendo aumentar la velocidad que puede alcanzar un tren y mejorando la frecuencia de los mismos. De esta manera, se ha conseguido acercar ciudades, permitiendo que los viajes entre éstas sean más rápidos y agradables.

Sin embargo, al aumentar la velocidad de un tren o al aumentar la frecuencia de paso, se generan una serie de amenazas y situaciones de riesgo que antes no existían.

Es por eso que la Seguridad Ferroviaria desempeña un papel fundamental en la señalización ferroviaria, permitiendo que el progreso en el transporte ferroviario se haga de una manera segura, evitando riesgos y sin poner a los viajeros en peligro.

1.2 Objetivos

El objetivo fundamental del presente proyecto es el de describir las actividades que son necesarias realizar para poder generar un Dossier de Seguridad para una aplicación específica en la que se quiera instalar el sistema de señalización ferroviaria. Este proyecto se centra en el sistema de señalización ERTMS (*European Railway Traffic Management System*) Nivel 1. En base a ese objetivo principal, se proponen los siguientes objetivos parciales:

- Explicar de manera resumida el funcionamiento del sistema de señalización ERTMS Nivel 1.

- Dar a conocer la normativa vigente en cuanto a proyectos de señalización ferroviarios relacionados con el *Safety.*

- Desarrollar las fases del ciclo de vida del sistema con el fin de obtener una instalación que se pueda considerar como segura.

1.3 Estructura del proyecto

El proyecto consta de 5 capítulos, siendo el primero de ellos la presente introducción y especificación de objetivos.

En el capítulo 2 se describen los principales elementos de la señalización ferroviaria y cuáles son los equipos imprescindibles que componen una línea para que pueda operar con seguridad en servicio comercial.

Además se explica más en profundidad el sistema ERTMS, en especial el nivel 1. Se habla de la funcionalidad de este sistema y de los equipos de vía necesarios para su implementación.

En el capítulo 3 se hace referencia a la normativa aplicable a los sistemas de señalización ferroviarios y se especifica en qué consiste la ingeniería RAMS a través de la cual se consigue que una instalación cumpla una serie de objetivos de seguridad. Se hace hincapié en la rama de Seguridad de la Ingeniería RAMS en las aplicaciones específicas ferroviarias.

En el capítulo 4 se detallan las fases del ciclo de vida incluidas en la normativa para poder construir un Dossier de Seguridad. Dentro de cada fase se desarrollan las actividades que el equipo de Seguridad o el Ingeniero de Seguridad deben realizar. Dichas actividades incluyen la generación de planes, la revisión de documentación de entrada al dossier, o la elaboración de informes de seguridad.

Por último, en el capítulo 5 se indican cuáles son las principales conclusiones obtenidas con la realización de este proyecto y las futuras líneas de desarrollo.

2. Señalización ferroviaria y Sistema ERTMS Nivel 1

En este capítulo se describen de manera resumida los principales elementos que componen los sistemas de señalización ferroviaria. A continuación; se describe el sistema de protección de tren ERTMS Nivel 1.

2.1 Sistemas de señalización ferroviaria

Un sistema de señalización ferroviaria es el conjunto de elementos y materiales destinados a obtener que el movimiento de los trenes se efectúe en condiciones de seguridad y sin accidentes.

La señalización en el ferrocarril es una parte vital del sistema ferroviario. Su evolución ha ido a la par a la evolución del ferrocarril. Hoy en día es la base de la seguridad en el movimiento de los trenes. Su importancia se ha ido incrementando progresivamente, de manera que, cualquier evolución del ferrocarril lleva unido la evolución de la señalización, como medio imprescindible de garantizar la seguridad y proporcionar las herramientas necesarias para regular el tráfico, de acuerdo con las demandas sociales.

Sus funciones son:

- Garantizar la seguridad en el movimiento de los trenes (Seguridad).
- Permitir el control del movimiento de los trenes (Control).
- Posibilitar la gestión del movimiento de los trenes (Operación).

La señalización es el método empleado para regular las circulaciones, dando prioridades a unas sobre otras, por ejemplo, prioridad de pasajeros frente a mercancías. Otro de los objetivos principales es evitar accidentes, para ello:

- Mantiene una distancia de seguridad entre dos trenes consecutivos.
- Salvaguarda el movimiento de los trenes en las bifurcaciones, desvíos y travesías.

- Regula el paso de los trenes de acuerdo con la densidad de servicio y la velocidad exigida.

- Ante el fallo de un componente de señalización, garantiza la seguridad en el movimiento de los trenes.

2.1.1 Elementos que componen un sistema de señalización ferroviaria

2.1.1.1 Elementos de detección de presencia de tren

2.1.1.1.1 Circuito de Vía (CV)

El circuito de vía detecta la presencia de un tren, o material en general, en una cierta sección de vía. Cuando cualquier material entra en la zona protegida por el circuito de vía, este informa de su estado de ocupación de forma inmediata al enclavamiento. En la Figura 2.1 se observan los dos posibles estados que puede presentar un circuito de vía.

Cuando el material abandona la zona protegida por el circuito, este informa de modo seguro al enclavamiento de que se ha desocupado el área del circuito de vía.

Los circuitos de vía de audiofrecuencia, llevan implícito una zona de solape (19 metros), de tal forma que en las situaciones donde hay señales enfrentadas, estas no se instalan juntas (cercanas), sino separadas como mínimo la zona de solape. Dentro de la zona de solape, existe una sub-zona, denominada zona muerta donde no se tiene detección y que debe ser lo más reducida posible.

Las funciones mínimas de seguridad que deberán tener los circuitos de vía de audiofrecuencia para cumplir los objetivos de seguridad son:

- Fallo del sistema, proceso que tiene el sistema de pasar a un estado seguro conocido al detectarse un fallo dentro de sí mismo. Esto se consigue aislando las salidas serie y paralelo conectadas a los elementos a controlar, dejando el circuito de vía en estado de ocupado.

- Autocomprobación, los microprocesadores utilizados en procesos vitales efectúan comprobaciones continuas de todos sus componentes: autocomprobación de la CPU, de las EPROMs, de las RAMs, convertidores, y resto de elementos implicados, para verificar su correcto funcionamiento. Las rutinas de autotest internas cíclicas permiten la detección de errores.

- Degradación parcial, cuando ocurre un fallo en cualquier entrada o salida vital, el sistema, la aísla. El aislamiento de entradas o salidas individualmente, permite que el sistema siga funcionando, quedando solamente limitado al efecto del fallo.

- Comprobación de interfaces entre módulos para garantizar una comunicación "segura", aunque dichas interfaces sean redundantes.

- Mecanismos de protección de los telegramas serie que se intercambian los distintos módulos, mediante códigos adecuados de protección de errores.

Aplicación:

El circuito de vía es el elemento básico para la detección de trenes en la vía. Un circuito de vía se compone de un equipo transmisor y uno o varios receptores. Cada uno tiene asociada una frecuencia, siendo distinta para los colaterales, para no interferirse en la detección.

Estados:

Los equipos de los circuitos de vía suministran al enclavamiento los estados Ref. [5]:

- Libre.- Estado que entrega cuando no hay ningún objeto cortando la señal del circuito de vía hasta el receptor.

- Ocupado.- Cuando se encuentra algún objeto en los carriles de la vía de tal manera que corte la señal hacia el receptor.

- Avería.- Aquellos Circuitos de Vía cuya tecnología lo permita, también ofrecerán al ENCE el estado de avería. A nivel lógico el tratamiento será el mismo que el de ocupado.

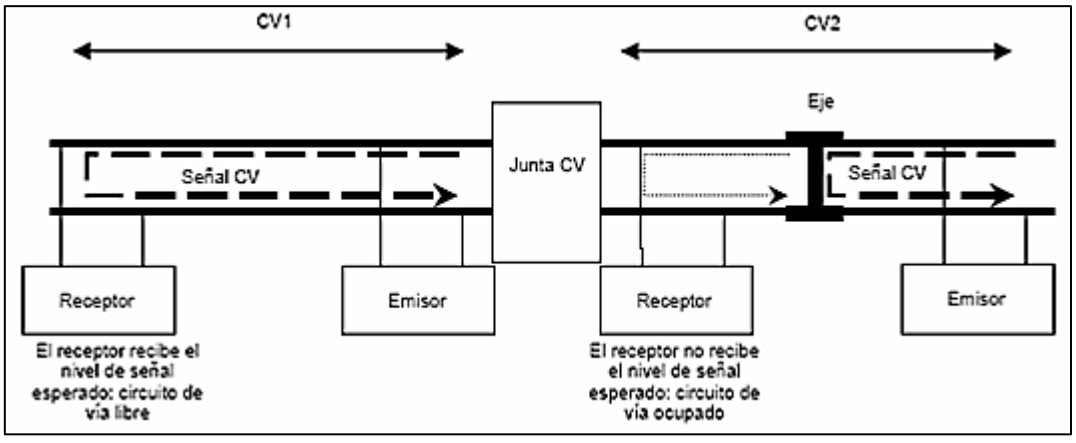


Figura 2.1 Ejemplo de detección de un tren. El circuito de vía 1 se encuentra libre mientras que el 2 se encuentra ocupado.

2.1.1.1.2 Contador electrónico de ejes

El contador electrónico de ejes es un elemento de localización del tren. El contador de ejes localiza al tren en una determinada sección de vía, por medio de contabilizar el paso de ejes. El enclavamiento recibe una información de ocupación / liberación de la sección de vía controlada, correspondiente al estado de ocupación de la zona de vía controlada por el contador, de forma segura. Ref. [5].

2.1.1.2 Señales laterales luminosas

La Tabla 2.1 presenta la simbología para los diversos aspectos presentados por las señales luminosas. Ref. [5].

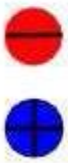
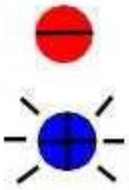
SIMBOLOGÍA DE ASPECTOS PARA LAS SEÑALES LUMINOSAS LATERALES	
Símbolo	**Descripción**
	Aspecto de vía libre (foco verde encendido fijo).
	Aspecto de anuncio de parada (foco amarillo encendido fijo).
	Aspecto de Anuncio de vía desviada (focos verde y amarillo encendidos fijos).
	Aspecto de parada (foco rojo encendido fijo).
	Aspecto de marcha limitada /itinerario a vía ocupada (focos rojo y blanco encendidos fijos).
	Aspecto de marcha limitada a mango (focos rojos y barra blanca encendidos fijos).
	Aspecto de ruta autorizada para trenes ERTMS N2 (focos rojo y azul encendidos fijos).
	Aspecto de ruta autorizada para trenes ERTMS N1 y 2 (foco rojo encendido fijo y foco azul encendido destellante).

Tabla 2.1 Simbología de aspectos para las señales luminosas laterales

2.1.1.2.1 Vía Libre

El tren está autorizado a pasar por la siguiente señal a máxima velocidad que permita la línea.

El aspecto que presentará la señal es foco verde fijo.

2.1.1.2.2 Anuncio de parada

La orden “anuncio de parada” indica al Jefe del tren que se debe detener en el próximo punto de parada, que coincide con la siguiente señal lateral luminosa. El aspecto que presentará la señal es el de foco amarillo fijo.

2.1.1.2.3 Anuncio de vía desviada

El “anuncio de vía desviada” indica al Jefe del tren que debe reducir su velocidad al pasar por el primer aparato de vía, y los siguientes, en posición desviada situados tras la siguiente señal.

Este aspecto se presenta cuando alguno, o algunos, de estos desvíos están en posición desviada.

El aspecto que presentará la señal en este caso es foco verde fijo – foco amarillo fijo.

2.1.1.2.4 Parada

La orden “parada” indica al Jefe del tren que debe detenerse frente a la señal que presenta dicho aspecto, siendo irrebasable, salvo por autorización expresa incluida en la reglamentación.

La señal presentará el aspecto de foco rojo fijo. En caso de que la señal esté apagada, el Jefe del tren entenderá que también está recibiendo la orden de parada.

2.1.1.2.5 Marcha limitada e itinerario a vía ocupada

El tren es autorizado a proceder con marcha limitada a partir de la señal hasta el límite de marcha limitada.

El aspecto que presentará la señal es foco rojo – foco blanco fijo.

Este aspecto es presentado por señales con rutas establecidas del tipo marcha limitada o itinerario a vía ocupada, en caso de que la ruta enclavada lo esté sobre una vía que no sea un mango.

2.1.1.2.6 Marcha limitada e itinerario a vía ocupada a mango

El tren es autorizado a proceder con marcha limitada a partir de la señal hasta el límite de marcha limitada.

El aspecto que presentará la señal es foco rojo – foco barra blanca fijo.

Este aspecto es presentado por señales con rutas establecidas del tipo marcha limitada, en caso de que la ruta enclavada lo esté sobre una vía que sea un mango.

2.1.1.2.7 Ruta autorizada para trenes ERTMS N2

Si el tren que se acerca a la señal está circulando en ERTMS nivel 2, el Jefe del tren podrá rebasar la señal, cuando el equipo de a bordo le dé la autorización de movimiento correspondiente. Este aspecto indicará parada absoluta a los trenes que no circulen al amparo de ERTMS N2.

La indicación que presentará la señal es foco rojo fijo + foco azul fijo.

2.1.1.2.8 Ruta autorizada para trenes ERTMS N1/2

La ruta autorizada permite el paso a trenes que circulen en ERTMS tanto en nivel 1, como en nivel 2. El aspecto indica que los trenes circulando en los niveles 1 o 2 de ERTMS pueden rebasar la señal haciendo caso al DMI (*Driver Machine Interface*), cuya indicación tiene preferencia sobre la señalización lateral.

El aspecto que presenta la señal es foco rojo fijo + foco azul destellante.

Los trenes que funcionen al amparo de ASFA o de la señalización lateral luminosa, deberán considerar que la señal les ordena parada absoluta (señal en rojo).

2.1.1.3 Desvíos

Las agujas o desvíos constituyen los elementos mecánicos que permiten cambiar de vía a los trenes. Estos elementos mecánicos están formados por una aguja flexible móvil (espadín) y, llegado el caso, de un corazón móvil cuya maniobra se efectúa por medio de motores eléctricos. Ref. [5].

La posición de estos elementos móviles se comprueba por los controladores que pueden estar integrados en los motores, o bien, ser independientes. Además, algunas agujas constan de sensores (pedales electrónicos) que permiten detectar un talonamiento en la propia aguja.

El talonamiento se produce cuando un tren acomete un desvío por la posición contraria a la que este está acoplado.

2.1.1.3.1 Posición del desvío

Se dice que una aguja está:

- En posición a izquierdas: si un tren que entre en la aguja por la punta o espadín toma la dirección a izquierda (ya sea esta general o desviada).

- En posición a derechas: si un tren que entre en la aguja por la punta o espadín toma la dirección a derechas (ya sea esta general o desviada).

Se dice que una aguja está:

- A normal (+): si el desvío está comprobando a posición general.
- A invertido (-): si el desvío está comprobando a posición desviada.

La Figura 2.2 muestra un desvío posicionado a normal:

Figura 2.2 Desvío posicionado a derechas (general, + o normal)

2.1.1.4 DCO (Detector de Caída de Objetos)

Los equipos de detección de caída de objetos son sensores que determinan la presencia de objetos en la vía y que, por lo tanto, pueden afectar a la seguridad de la circulación de los trenes. La información es procesada por un ordenador que se encuentra en el edificio técnico o caseta técnica más cercana. Este ordenador manda, a su vez, los datos al centro de control CRC. Ref. [5].

2.1.1.5 Enclavamiento Electrónico

La función básica del enclavamiento electrónico es controlar el accionamiento de los elementos situados en la vía (señales, cambios de aguja, pasos a nivel, etcétera) asegurando que se cumplan las relaciones de dependencia, el orden de accionamiento y cualquier otra restricción necesaria para garantizar la seguridad en la circulación de trenes en cualquier circunstancia.

A lo largo de la historia del ferrocarril se han realizado los enclavamientos con las tecnologías disponibles en cada momento, desde sistemas puramente mecánicos, hasta llegar recientemente a los sistemas electrónicos controlados por procesadores, pasando por los relés electromecánicos. Ref. [5].

2.1.1.6 CTC (Control de Tráfico Centralizado)

El CTC surge de la necesidad de tener una visión de conjunto de la posición de los trenes, así como de la disposición en cada instante de los desvíos y las rutas establecidas, para poder actuar sobre los mandos de señales e itinerarios y regular adecuadamente el tráfico en una zona específica.

Los CTC permiten el mando y la regulación de un área extensa desde un único punto, es parte integrante del sistema de mando y control (CRC).

Desde el CTC se mandan los itinerarios, se regula el tráfico, y se resuelven todos los posibles conflictos operacionales de la circulación de los trenes, además genera información para los viajeros, como horas de llegada o posibles desviaciones de los horarios.

El CTC manda las órdenes a los enclavamientos, responsables estos de la seguridad, y recibe de ellos la confirmación de estas órdenes y la información referente a la situación de los trenes y al estado de la vía. Ref. [5].

En la
Figura 2.3 se muestra una imagen de un puesto de Control de Tráfico Centralizado.

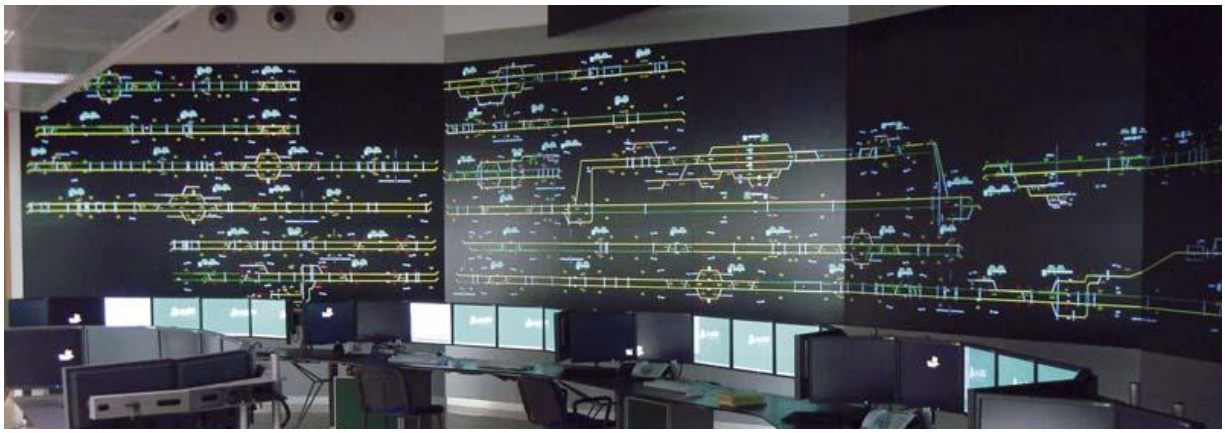


Figura 2.3. Imagen de un CTC

2.1.2 Sistemas de protección de tren

2.1.2.1 Sistema ASFA

El sistema de Anuncio de Señales y Frenado Automático (Sistema ASFA) está constituido por dos conjuntos de equipos:

- Uno instalado en vía: ASFA VIA.
- El otro va embarcado a bordo del material rodante: ASFA BORDO.

2.1.2.1.1 Balizas ASFA

Las balizas ASFA son dispositivos estáticos y pasivos, que envían la información del aspecto de la señal al paso del tren. La baliza no necesita alimentación para transmitir los datos al tren (de hecho, es la antena del tren la que proporciona la energía en forma de radiación electromagnética). Se necesita información eléctrica para que seleccione el código que debe enviar al tren. Ref. [9].

La baliza consiste básicamente en un circuito eléctrico resonante LC (bobina – condensador). Es posible seleccionar 5 frecuencias (se utilizan 4) por medio de la información que se procesa desde la señal. Estas frecuencias son:

- L1 (60000Hz): la señal presenta aspecto de anuncio de precaución (verdeamarillo) o anuncio de parada (amarillo).

- L3 (68310Hz): la señal presenta el aspecto de vía libre.

- L7 (88540Hz): la señal presenta el aspecto de parada, rebase autorizado, o marcha autorizada a trenes ERTMS, y la baliza que presenta este código es la baliza previa.

- L8 (95500Hz): la señal presenta el aspecto de parada, rebase autorizado, o marcha autorizada a trenes ERTMS, y la baliza que presenta este código es la baliza de pie de señal.

El sistema de captación, que consiste básicamente en un oscilador que conectado al captador, oscila a una frecuencia denominada FP (Frecuencia Permanente).

Cuando el captador pasa sobre una baliza, el oscilador pierde la frecuencia 21 y pasa a oscilar a la frecuencia de resonancia del circuito de la baliza, con la que sintoniza mediante acoplamiento inductivo, recibiendo la información del aspecto de la señal asociada a ésta.

2.1.2.2 LZB

El LZB (traducido, Control Lineal del Tren), desde el punto de vista de la transmisión, utiliza cable radiante ubicado en la caja de la vía que envía información al tren con frecuencias de 36 KHz. Esta señal es recibida por el tren a través de una antena captadora bajo el vehículo que, a su vez, emite también datos hacia la vía a 56 KHz.

Cada una de las centrales LZB tiene memorizado todos los perfiles de la línea con las limitaciones de velocidad permanentes, variables y temporales, así como información sobre posición de desvíos, ocupación de circuitos de vía, etc. Toda esta información es transmitida, a través de un cable instalado a lo largo de la vía, a los trenes y locomotoras, cuyo equipo a bordo procesa y aplica la curva de frenado correspondiente para adecuar la velocidad en cada punto. Ref. [9]

2.1.2.3 CBTC

En el sistema CBTC (Control de Trenes Basado en Comunicaciones), los trenes circulantes son los que comunican a los equipos de vía su estado (posición, velocidad, sentido de marcha, distancia de frenado, etc.) lo que permite calcular la zona potencialmente ocupada por el tren durante su marcha. Con esta información, los equipos de vía pueden calcular los puntos que no deben ser sobrepasados por otros trenes que circulen por la misma vía y se los transmite para que ajusten su velocidad y circulen con total seguridad. Con un símil automovilístico, los trenes reciben constantemente información de su distancia respecto al tren precedente y pueden ajustar su distancia de seguridad en consecuencia.

Por sus características, los sistemas CBTC permiten optimizar el uso de la infraestructura ferroviaria y alcanzar la máxima capacidad de transporte y el mínimo intervalo posible entre trenes compatible con una operación segura. Aunque su empleo es muy habitual en nuevas líneas de metro de alta demanda, es cada vez más frecuente que los operadores consideren su implementación en líneas ya existentes con objeto de mejorar su capacidad de transporte. Ref. [9].

2.1.2.4 ERTMS

El ERTMS (*European Rail Traffic Management System*) es un sistema de señalización en cabina y de control de trenes que surge con la motivación de proporcionar un estándar paneuropeo para facilitar la interoperabilidad entre diferentes países ERTMS está compuesto por dos componentes principales: El ETCS y el GSM-R.

2.1.2.4.1 ETCS (*European Train Control System*)

El ETCS es un sistema de control de trenes compuesto por el subsistema del tren y el subsistema de vía. Ref. [4].

ETCS realiza las funciones de control de los trenes, y consta de tres niveles:

- ETCS Nivel 1, (Figura 2.4) utiliza la transmisión puntual de información al tren por medio de transpondedores pasivos. También se usa la transmisión semicontinua por medio de lazos. Se trata de una tecnología suplementaria para la señalización lateral preexistente en líneas con baja o moderada intensidad de tráfico. Los cantones están definidos por el sistema de señalización ya instalado. Este nivel incrementa la seguridad en el caso de señalización temporal de precaución y en áreas de restricción de velocidad. Adicionalmente la señalización en cabina permite incrementar la velocidad de la línea.

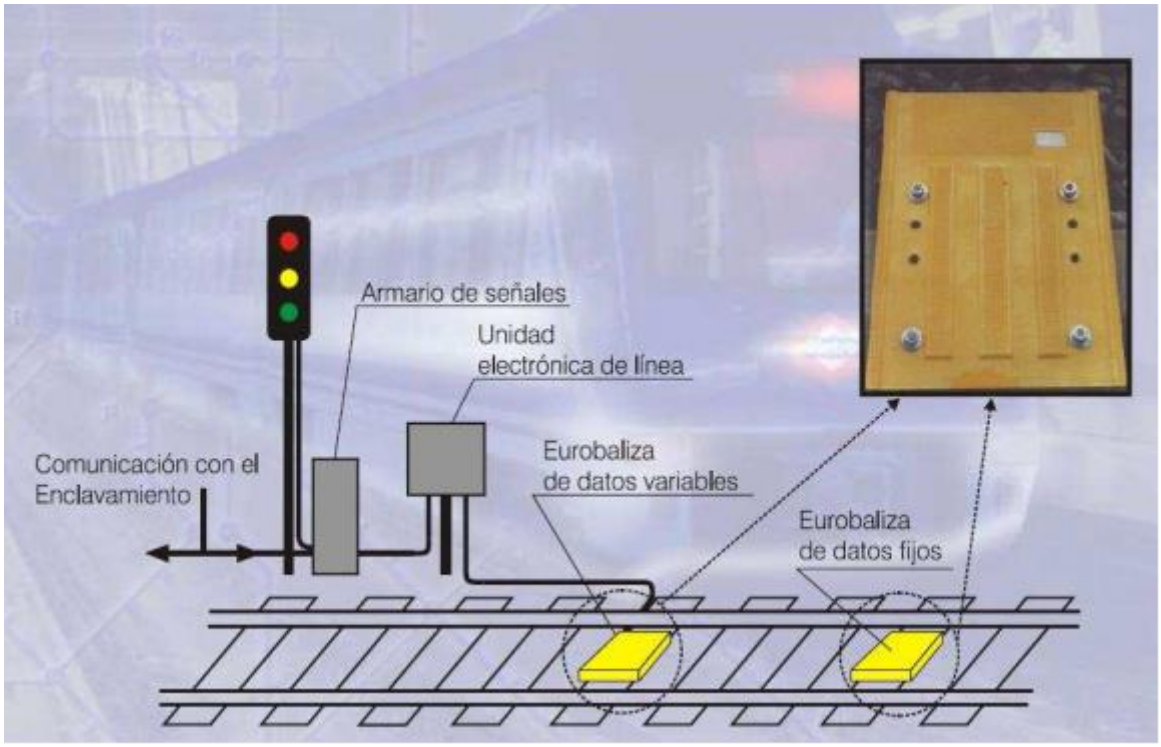


Figura 2.4. Arquitectura sistema ETCS Nivel 1

- ETCS Nivel 2, como el Nivel 1, puede instalarse "por encima" de un sistema anterior de señalización luminosa. Las señales fijas pueden ser total o parcialmente sustituidas por señalización en cabina. El RBC (*Radio Block Center*) traza la localización de cada tren controlado dentro de su área. EL RBC determina y transmite una descripción de la vía y autoriza los movimientos, de forma individualizada para cada tren controlado, de acuerdo con el sistema de señalización subyacente. Adicionalmente ofrece al RBC los datos del tren en especial su posición. Puede incrementarse la velocidad, ya que el RBC puede inspeccionar varios cantones.

- ETCS Nivel 3 presenta adicionalmente funciones tales como la determinación activa de la distancia entre los trenes. No es necesaria la existencia de un sistema de monitorización lateral, puesto que los trenes informan de manera activa sobre su posición al centro de control, desde el comienzo de la composición hasta el último de los vagones. Para incrementar la capacidad de las líneas puede instaurarse el sistema de cantones móviles. La principal ventaja del nivel 3 consiste en la reducción de costes de amortización por la sustitución de los elementos de monitorización de ocupación de vía y de la señalización lateral.

2.1.2.4.2 GSM-R

El sistema GSM-R es un sistema de comunicaciones vía radio para proporcionar enlace de voz y datos entre la vía y el tren, basado en el estándar GSM.

GSM-R se encarga de la transmisión de voz y datos entre el tren y las instalaciones fijas. Este sistema es similar a los sistemas GSM públicos en cuanto a arquitectura de red, pero utiliza una banda de frecuencias separada y proporciona servicios exclusivos para el ámbito ferroviario: llamadas de grupo, llamadas de emergencia, numeración funcional, etc. Ref. [4].

2.2 ERTMS Nivel 1

2.2.1 Descripción del sistema

El sistema ERTMS constituye el sistema de protección de tren interoperable acordado entre los diferentes suministradores de equipos de señalización europeos y las distintas administraciones ferroviarias europeas.

Con el objetivo de definir las especificaciones técnicas y funcionales del sistema se ha creado UNISIG (*Union Industry of Signalling*), compuesto por las siguientes empresas:

Alcatel (Thales) – Alstom – Bombardier TS – Invensys -Siemens

El objetivo de la especificación es el establecer los elementos necesarios para conseguir la interoperabilidad técnica de todos los equipos sea cual fuere el fabricante de los mismos. En un nivel más avanzado se consigue la interoperabilidad funcional, consistente en unificar las funcionalidades llevadas a cabo con las herramientas que nos aporta el sistema.

La figura
Figura 2.5 muestra la arquitectura general de un sistema ERTMS Nivel 1.

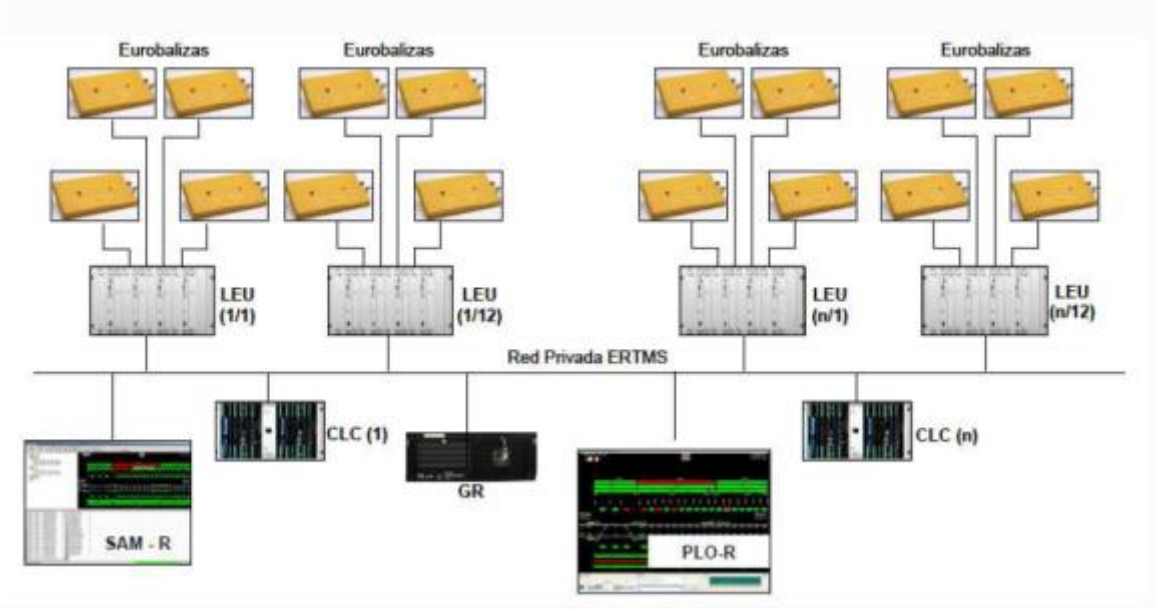


Figura 2.5. Arquitectura general de un sistema ERTMS Nivel 1

2.2.1.1 Controlador Centralizado de LEUs (CLC)

El objetivo del controlador centralizado de LEUs es proporcionar un medio de gobernar de forma centralizada los elementos de nivel 1 de la estación. Para ello el controlador centralizado de LEUs recibe la información de señalización desde el ENCE de forma segura y la distribuye a los LEUs que tiene conectados, que a su vez se encargan de enviar los telegramas a sus respectivas Eurobalizas conmutables. Ref. [9].

Las tareas del controlador centralizado de LEUs consisten en lo siguiente:

- La recepción de informaciones del enclavamiento sobre:

    1. Aspectos de las señales

    2. Estado de las agujas.

- Distribución continua de la información del ENCE a los LEUs:

    Envía a cada LEU la parte que necesita de la información de señalización. De esta forma el LEU puede seleccionar dentro de su tabla de telegramas preprogramados, los telegramas que en cada momento debe enviar a sus balizas.

- Supervisión del estado de los LEUs.

- Envío de la información de diagnosis al Sistema de Ayuda al Mantenimiento.

2.2.1.2 LEU (Codificador de balizas)

La interacción con las balizas se realiza mediante los LEUs. A través de este módulo, se envían las ordenes (telegramas) a las balizas. Un LEU es un ordenador redundante, trabajando en modo 2 de 2 e intrínsecamente seguro en cuanto a señalización.

Un LEU puede controlar varias balizas, según la configuración necesaria. Las informaciones son en este caso independientes entre sí, es decir, a cada baliza se le pueden asignar señales diferentes. Ref. [7].

Las tareas del LEU consisten en lo siguiente:

- Recibir información de señalización desde el CLC.
- Recibir información de las Limitaciones Temporales de Velocidad LTVs desde el GR.
- Seleccionar dentro de la tabla activa de telegramas preprogramados, los telegramas a enviar a las balizas en base a la información recibida del CLC.
- Cambiar de tabla activa de telegramas preprogramados, bajo petición del GR.
- Enviar el estado de funcionamiento al CLC.
- Enviar información de diagnosis al SAM-R local.
- Enviar los telegramas a las balizas.
- Supervisión continúa del interface con el CLC.

2.2.1.3 Eurobalizas

La eurobaliza (Figura 2.6) es un dispositivo de campo, que al paso del tren sobre ella es energizada por la antena del tren, enviando el telegrama programado al equipo de a bordo. El telegrama enviado es el que selecciona el LEU (en el caso de las eurobalizas conmutables). Ref. [7].

Los trenes equipados con el sistema ETCS necesitan disponer de forma precisa de su ubicación en la línea. Dado que los sistemas de odometría no son absolutamente precisos, sobre todo a altas velocidades, es necesario corregir las discrepancias entre la ubicación calculada y la real de forma regular. Para ello se utilizan las llamadas marcas de localización (eurobalizas fijas).

Se equiparán dos tipos de balizas en vía:

- **Balizas fijas**: Se utilizan para enviar información que no varía al cambiar la señalización (como por ejemplo gradientes) y para relocalización, es decir, mandan siempre el mismo telegrama, que transmiten al equipo embarcado

ETCS del vehículo cuando este circula sobre ellas. Por ello no están conectadas al LEU pues transmiten siempre la misma información.

- **Balizas conmutables**: Pueden mandar telegramas diferentes, seleccionados por el LEU, que contienen, en la mayor parte de los casos, perfiles de velocidad, autorizaciones de movimiento y condiciones de vía. La referencia de localización en el nivel 1 se produce fundamentalmente mediante las distancias de enlace entre grupos de balizas, comparando dicha distancia con la medición de recorrido en el vehículo.

Figura 2.6. Eurobalizas de los distintos fabricantes

2.2.1.4 Sistema de Control ERTMS

ERTMS es un sistema completo que proporciona funciones diferentes, algunas de ellas pueden ser realizadas por componentes ERTMS estándar. Pero hay otras funciones que no se pueden asignar a un producto completo y que han de ser realizadas por un conjunto de equipos y una serie de procedimientos asociados, como es el caso del Sistema de Control (Figura 2.7).

El Sistema de Control ERTMS es un sistema necesario en aplicaciones ERTMS donde se implemente la Gestión de Limitaciones Temporales de Velocidad (Nivel 1 y Nivel 2). El proceso de LTV, de acuerdo con las especificaciones de UNISIG (lenguaje ERTMS),

genera los datos de configuración para los LEUs cuando el usuario desea introducir / anular limitaciones temporales de velocidad.

Por tanto, este sistema se desarrollará para obtener del operador los comandos que permiten activar o desactivar una LTV y llevar a cabo las gestiones necesarias para ello. Ref. [7].

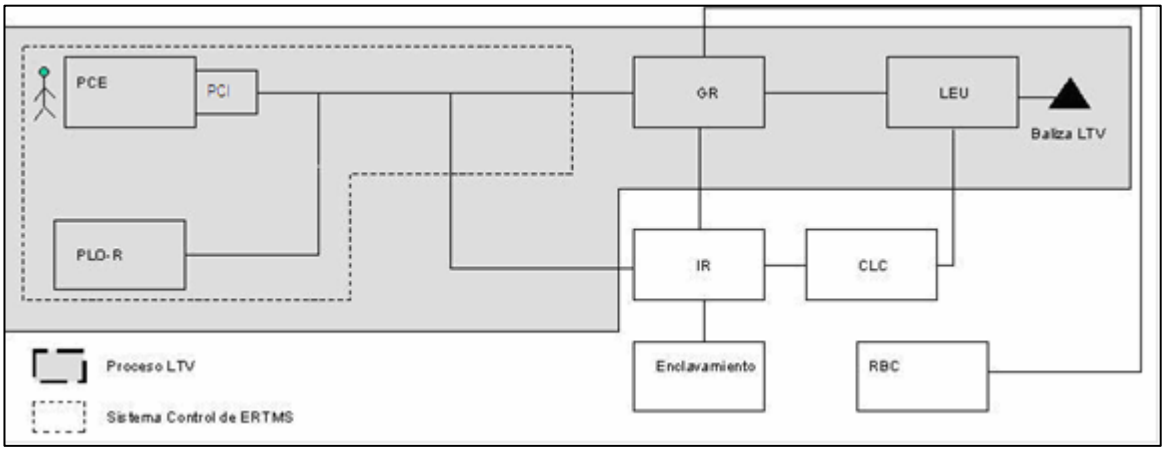


Figura 2.7. Ejemplo de arquitectura de equipos de un sistema de control ERTMS

2.2.1.4.1 Puesto Local de Operaciones ERTMS (PLO-R)

El PLO-R es un ordenador que realiza la gestión del Sistema ERTMS. Se trata de un Puesto Local de Operación que permite al operador realizar las siguientes funciones (Figura 2.8):

- Establecimiento y anulación de LTVs estáticas y/o dinámicas.

- Visualización del estado de los elementos del sistema ERTMS.

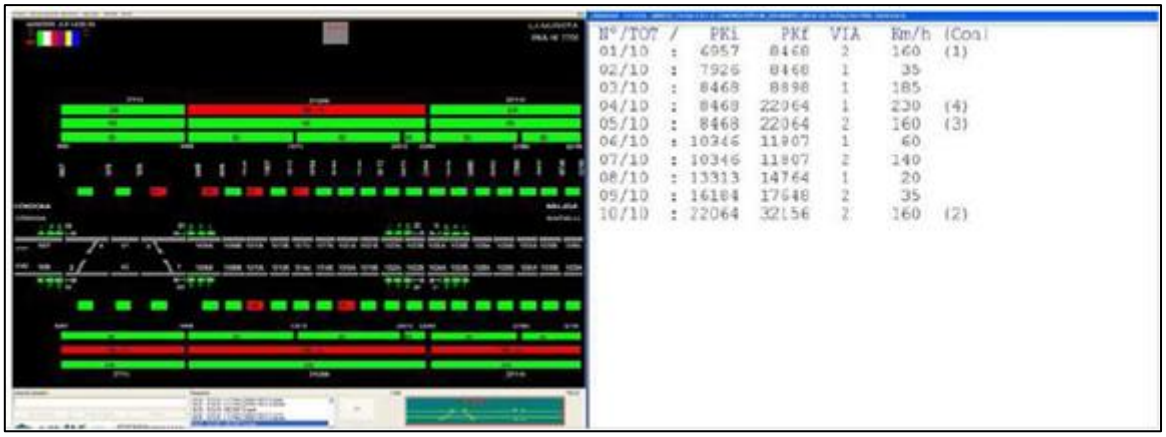


Figura 2.8. Ejemplo de interface gráfico de un PLO-R

2.2.1.4.2 Gestor de ERTMS (GR)

El Gestor de ERTMS (GR) es un sistema que gestiona la aplicación / anulación de las Limitaciones Temporales de Velocidad estáticas y dinámicas.

El GR no tiene interface de usuario, es decir, no dispone de monitor, teclado y ratón. Utiliza un software diverso, ya que dispone de un proceso que se encarga de generar las tablas de telegramas con las LTVs para sus LEUs asociados, y otro proceso que analiza el contenido de estas tablas para que el operador confirme si quiere o no cambiar el estado de las LTVs conforme a las tablas que se acaban de generar.

2.2.1.4.3 Puesto Central de ERTMS (PCE)

El PCE es un Puesto de Operaciones que gestiona las aplicaciones de control de ERTMS de forma centralizada. El Puesto Central de ERTMS permite al operador realizar las siguientes funciones (Figura 2.9):

- Establecimiento y anulación de LTVs estáticas y dinámicas.

- Visualización del estado de los elementos del sistema ERTMS.

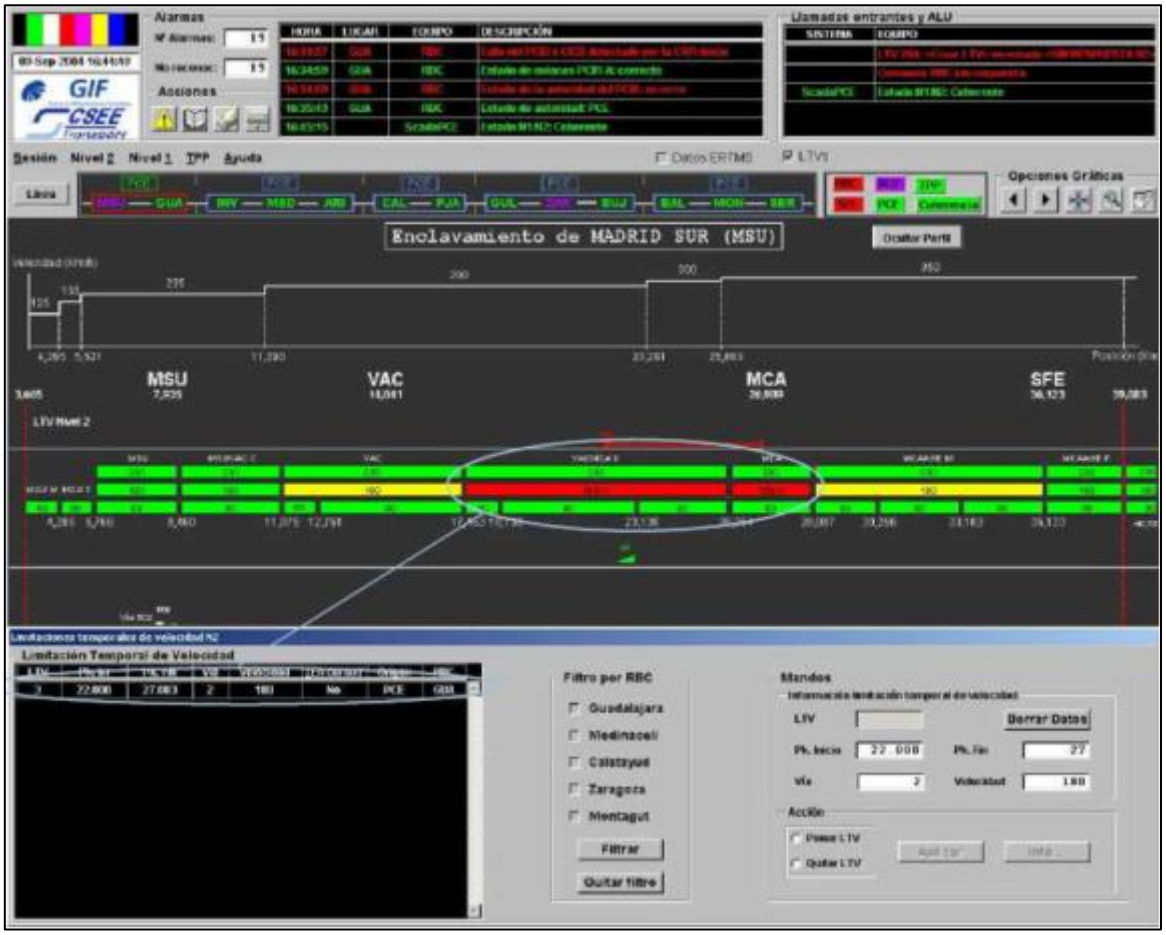


Figura 2.9. Ejemplo de Interface Gráfico de un PCE.

2.2.1.4.4 PC de comunicaciones intermedio (PCI-R)

El PCI-R es un ordenador a través del cual el Puesto Central de ERTMS (PCE) se comunica con los equipos locales, conectados a la Red Privada de Señalización, consiguiendo así el aislamiento de las redes de comunicación. Se instala en configuración duplicada, por motivos de disponibilidad.

2.2.2 Niveles de funcionamiento

El sistema está estructurado en diferentes niveles de aplicación que establecen diferentes maneras de establecer la comunicación entre el nivel de vía y el tren. La definición de los niveles está relacionada con el equipamiento en vía utilizado para enviar la información al tren y las funciones asociadas a cada uno de ellos. Un tren equipado con el sistema ERTMS estará en cada momento en el correspondiente nivel de funcionamiento en función del equipamiento en vía presente y disponible. Así mismo se han establecido los criterios para la realización de las transiciones entre los distintos niveles. Es posible la superposición de niveles de funcionamiento en la misma línea, en función del equipamiento de los trenes.

Los niveles 1, 2 y 3 son compatibles en sentido descendente. Es decir, un tren equipado con nivel 3, puede circular en líneas equipadas con nivel 2 o 1, uno equipado con nivel 2 lo puede hacer en una línea equipada exclusivamente con nivel1. Ref. [3].

2.2.2.1 Nivel 0

El Nivel 0 es el nivel de funcionamiento utilizado para un tren equipado circulando en una línea sin equipamiento ERTMS.

La conducción del tren estará basada en sistemas de señalización lateral. El sistema ERTMS solamente realiza la supervisión de la velocidad máxima definida para el modo UN (*unfitted*). Al maquinista no se le enviará ningún otro tipo de información. La detección del tren y la supervisión de su integridad están aseguradas por el enclavamiento y los circuitos de vía. Estos sistemas se encuentran fuera del ámbito del ERTMS.

Equipamiento y funciones requeridos en vía:

1. No existirá equipamiento en vía a excepción de alguna eurobaliza para anunciar la transición a otro nivel o algún comando específico.

2. No existen funcionalidades implementadas en vía relativas al sistema ERTMS.

Equipamiento y funciones requeridos en el equipo embarcado:

1. Equipo embarcado con equipamiento de lectura de eurobaliza.

2. Funciones ERTMS Embarcadas:

- Supervisión de la máxima velocidad del tren.

- Supervisión de máxima velocidad en zona UN.

- Lectura de eurobalizas para transición y comandos especiales.

2.2.2.2 Nivel 1

El Nivel 1 (Figura 2.10) es el nivel de funcionamiento utilizado para un tren equipado en una línea con sistema de transmisión por eurobalizas.

Es necesaria la existencia de un sistema de enclavamiento como sistema básico de señalización. Las autorizaciones de movimiento son generadas por el sistema de suelo y son enviadas al tren a través de eurobalizas.

Aun tratándose de un sistema de transmisión puntual, la supervisión de la velocidad del tren y del límite de la autorización es continua.

Deberá existir un sistema de enclavamiento y detección de presencia e integridad de tren, fuera del ámbito del sistema ERTMS. La señalización lateral es necesaria para reanudar la marcha siempre que no exista un dispositivo *infill* continuo.

Equipamiento y funciones requeridos en vía:

1. Eurobalizas para la transmisión de información al tren. Podrán ser fijas para enviar información invariable o conmutables para el caso de información variable según las condiciones de vía.

2. Transmisión de la autorización de movimiento en función de las condiciones de enclavamiento de vía establecidas por el enclavamiento.

3. Envío de informaciones complementarias de descripción de vía necesarias para la gestión del movimiento del tren.

Equipamiento y funciones requeridos en el equipo embarcado:

1. Equipo embarcado con equipamiento de lectura de eurobaliza.

2. Funciones ERTMS embarcadas.

3. Recepción de la autorización de movimiento y descripción de la vía transmitida por las eurobalizas.

4. Selección de la velocidad más restrictiva en cada punto.

5. Cálculo de la curva de velocidad teniendo en cuenta las características de frenado y aceleración del tren así como la descripción de la vía.

6. Comparación de la velocidad del tren con la velocidad permitida y mando del freno si es necesario.

7. Información al maquinista.

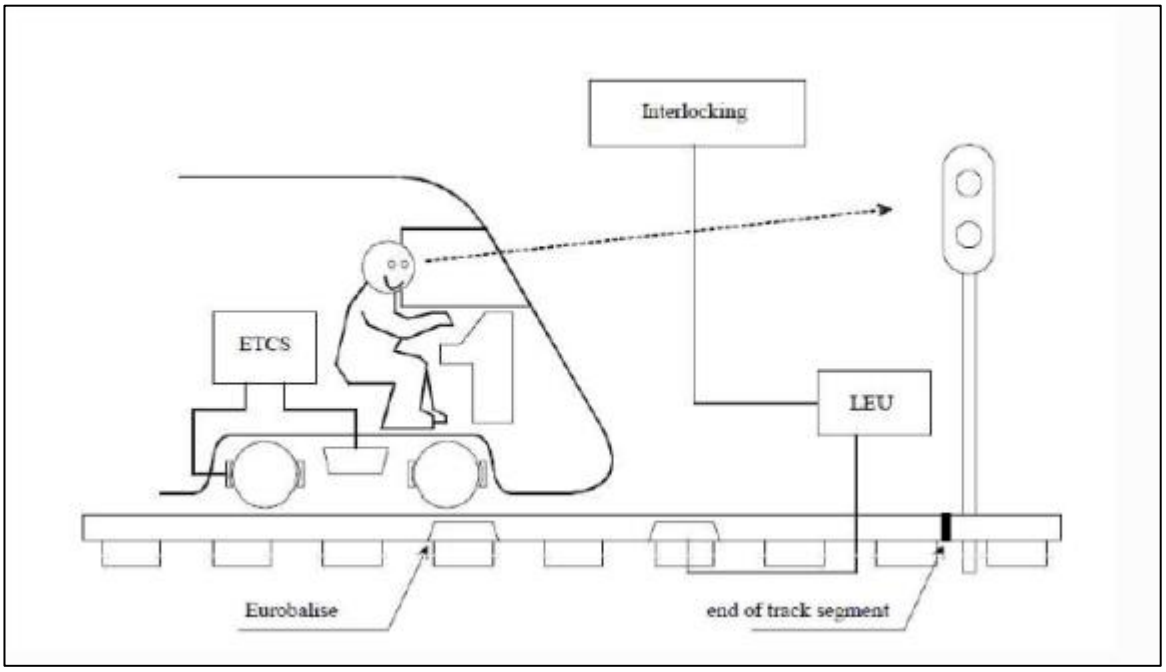


Figura 2.10. ERTMS N1. Equipamiento vía-tren

2.2.2.3 Nivel 2

El Nivel 2 es el nivel de funcionamiento utilizado para un tren equipado en una línea controlada por el *Radio Block Centre* (RBC), transmisión continua por radio GSM-R y eurobalizas de posicionamiento (Figura 2.11). La localización del tren y su integridad están garantizadas por el sistema de detección de tren (circuito de vía).

Es necesaria la existencia de un sistema de enclavamiento como sistema básico de señalización.

Las autorizaciones de movimiento son generadas por el sistema de suelo y son enviadas al tren a través del sistema de euroradio GSM-R. Es, por lo tanto, un sistema de transmisión continuo con supervisión continua.

Será necesaria la presencia de un sistema de detección de tren y garantía de integridad del mismo, fuera del ámbito del ERTMS.

El RBC suministra información al tren en cada momento de forma individualizada conociendo la identidad de cada uno de los trenes que tiene bajo su control.

La señalización lateral en este caso no es necesaria.

Equipamiento y funciones requeridos en vía:

1. Radio Block Centre (RBC).

2. Euroradio GSM-R para transmisión de información bidireccional.

3. Eurobalizas fundamentalmente para relocalización del tren.
4. Conocimiento de los trenes controlados dentro de cada zona.

5. Seguimiento de los trenes que se encuentran bajo control.

6. Determinación de la autorización de movimiento para cada uno de los trenes según la situación del enclavamiento.

7. Transmisión de la autorización de movimiento y la descripción de la vía de forma individual para cada tren.

8. Gestión de las transiciones entre RBCs.

Equipamiento y funciones requeridos en el equipo embarcado:

1. Equipo embarcado con equipamiento de lectura de Eurobaliza.

2. Equipo euroradio GSM-R.

3. Lectura de eurobaliza y envío al RBC de la posición relativa respecto a ella.

4. Recepción vía euroradio de la autorización de movimiento referido a la eurobaliza.

5. Selección de la velocidad más restrictiva en cada punto.

6. Cálculo de la curva de velocidad teniendo en cuenta las características de frenado y aceleración del tren así como la descripción de la vía.

7. Comparación de la velocidad del tren con la velocidad permitida y mando del freno si es necesario.

8. Información al maquinista.

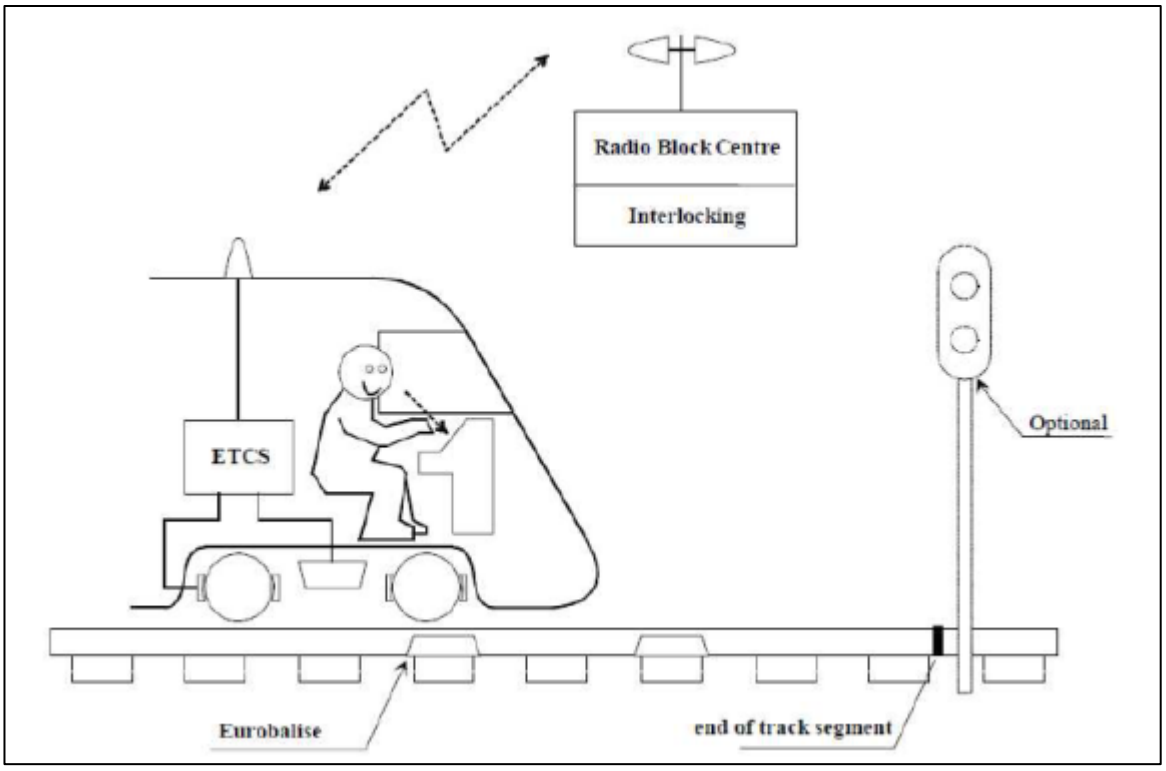


Figura 2.11. ERTMS N2. Equipamiento vía-tren

2.2.2.4 Nivel 3

El Nivel 3 es el nivel de funcionamiento utilizado para un tren equipado en una línea controlada por el *Radio Block Centre* (RBC), transmisión continua por radio GSM-R y eurobalizas de posicionamiento. En este caso la localización del tren y su integridad está garantizada por el equipo embarcado y el RBC.

2.2.3 Principios básicos ERTMS N1

La configuración de un grupo de balizas es:

- Un grupo de balizas está constituido como máximo por ocho eurobalizas.
- Cada eurobaliza tendrá información de su posición interna dentro del grupo, del número de balizas del grupo y la identidad del grupo.
- El número de cada eurobaliza describe la posición dentro del grupo.
- La referencia de posición de un grupo corresponde con el eje de la eurobaliza número 1.

- La dirección nominal de un grupo de balizas viene dado por el sentido creciente en orden de eurobalizas.

- En nivel 1, en los grupos consistentes en una sola baliza, el sentido viene determinado por la información de enlace

- Una eurobaliza puede contener información válida para el sentido nominal, el inverso o ambos.

- La información envidada podrá ser normal o del tipo infill.

- Toda la información de distancia enviada desde un grupo de balizas lo hace respecto a la referencia del mismo.

- En el caso de información infill, la distancia se referirá al punto de referencia del grupo principal al que pertenece la información.

- El conjunto de telegramas enviado por un grupo se denomina mensaje.

- Se considera perdida la lectura de una baliza dentro de un grupo si:

    1. No se lee una baliza en la distancia máxima desde le última lectura de baliza del grupo.

    2. Se produce un salto en el orden de lectura de balizas dentro del grupo.

2.2.3.1 Enlace

El objeto de la funcionalidad de enlace es el siguiente (Ref. [3]):

- Determinar si un grupo de balizas no se ha leído o lo ha sido fuera de la ventana de expectación tomando la acción adecuada en cada caso.

- Determinar el sentido de lectura en el caso de grupos de balizas simples.

- Corregir la posición del tren debido a los errores de odometría.

La información de enlace se compone de:

- La identidad del grupo enlazado.

- Posición del grupo enlazado, en distancia relativa.

- La precisión de la medida de dicha distancia.

- Dirección en la que se pasará por el grupo enlazado.

- Reacción prevista en caso de problemas de consistencia de lectura del grupo enlazado: *TRIP*, freno de servicio o sin reacción.

Pueden existir grupos no enlazados, pero deberán estar formados por al menos dos eurobalizas y estar identificados como tal.

Cuando se dispone de información de enlace:

- Sólo son tenidos en cuenta los grupos que se encuentran en la información de enlace y que se encuentran marcados como enlazados, siempre que se encuentren dentro de la ventana de expectación.

- La ventana de expectación tendrá en cuenta la precisión de enlace, el error de odometría y la posición de la antena respecto al tren.

- Si se dispone de información de enlace, se rechazará el mensaje de un grupo presente en la lista de enlace y se aplicará la reacción de enlace si se produce alguno de los siguientes hechos:

    1. Una baliza se pierde dentro del grupo

    2. Una baliza es leída pero el telegrama no puede ser decodificado

    3. Hay variables dentro del mensaje con valores no válidos

- Si el grupo está enlazado pero no se encuentra en la información de enlace presente en el tren en este momento, el mensaje se rechazará y no se aplicará reacción en caso de errores.

- Si no se dispone de información de enlace, el equipo embarcado rechazará el mensaje de un grupo marcado como enlazado y aplicará el freno de servicio si:

    1. Una baliza se pierde dentro del grupo

    2. Una baliza es leída pero el telegrama no puede ser decodificado

    3. Hay variables dentro del mensaje con valores no válidos.

2.2.3.2 Localización y posición del tren

El posicionamiento del tren en cada momento deberá tener en cuenta un intervalo de confianza basado en el error de odometría y en la precisión del enlace. Ref. [3].

- La ventana de posicionamiento del tren, aumenta en relación a la distancia recorrida desde la última relocalización en función del error de odometría.

- La ventana de posicionamiento se resetea al paso por un grupo enlazado.

- A partir de la ventana de posicionamiento se determinan tres puntos

    1. Posición estimada del tren (*Estimated Front End*). Correspondiente con la posición calculada en cada momento para la cabeza del tren.

    2. *Max. Safe Front End*. Correspondiente con la posición más adelantada teniendo en cuenta la ventana de posicionamiento.

    3. *Min. Safe Front End*. Correspondiente con la posición más retrasado teniendo en cuenta la ventana de posicionamiento.

- El equipo embarcado podrá mostrar al maquinista bajo petición la posición kilométrica estimada para la cabeza del tren con una resolución de 1 metro.

- El equipo de suelo enviará información geográfica de manera que la distancia máxima entre puntos de información geográfica de referencia no exceda de 10 km.

2.2.3.3 Autorización de movimiento

Para el control del movimiento del tren, este deberá recibir las siguientes informaciones por parte del equipamiento de vía:

- Autorización de movimiento (MA), expresado en distancia permita a recorrer desde el punto de información.

- Información de enlace.

- Descripción de la vía en la distancia cubierta por el MA, con las siguientes informaciones posibles:

    1. Perfil estático de velocidad.

    2. Perfil de gradiente.

    3. Limitaciones temporales de velocidad en caso de que haya alguna activada.

- Si el equipo embarcado recibe nueva información de descripción de la vía e información de enlace, esta reemplazará a la existente a partir del punto de comienzo de la nueva información.

- La información de MA contendrá los siguientes elementos:

    1. Localización del final de la autorización de movimiento EOA.

2. Velocidad al final de la autorización. Normalmente será cero, excepto en casos como el de salida de la línea.

3. Localización del punto a proteger más allá del EOA.

4. Velocidad de liberación. Es la velocidad a la que se permite circular el tren en la proximidad del EOA garantizando la protección del DP. Puede ser un valor fijo o calculada por el equipo embarcado.

5. El MA puede estar dividido en secciones y cada una de ellas con un temporizador asociado, de forma que la autorización está limitada en el tiempo sin que el tren disponga de la misma de forma infinita.

- Los temporizadores enviados en el MA arrancan en el momento de la lectura de la primera baliza del grupo, tanto si es grupo principal como *infill* (previo).

- Un nuevo MA, incluida su información asociada, reemplaza al existente, con esto se puede alargar o recortar una autorización existente.

2.2.3.4 Restricción de velocidad

Existen distintas causas, independientes entre sí, por las que la velocidad de circulación del tren puede estar restringida:

- Perfil estático de velocidad (*Static Speed Profile SSP*). Relacionado con condiciones permanentes de la infraestructura y dependientes del tipo de tren (categorías).

- Limitación temporal de velocidad (*Temporary Speed Restriction TSR*). Aplica una limitación de velocidad que no es permanente por condiciones de vía o trabajos.

- Velocidad máxima del tren. Es una limitación inherente al tren y no forma parte de la información enviada desde el equipamiento de vía.

- Restricción de velocidad ligada a la señalización. Utilizado para indicar la velocidad máxima o cero en el caso de señal cerrada.

- Limitación de velocidad por modo. Cada modo de funcionamiento tiene una velocidad asociada.

El denominado MRSP (*Most Restrictive Speed Profile*) corresponde con el perfil de velocidad más bajo calculado por el equipo embarcado teniendo en cuenta todas las restricciones de velocidad presentes mencionadas anteriormente.

2.2.3.5 LTVs de Nivel 1

Las Limitaciones Temporales de Velocidad (LTV) son restricciones de carácter temporal que se imponen en un tramo de vía por alguna razón excepcional, como por ejemplo la realización de trabajos que implican la presencia de personal en la propia vía o en sus proximidades.

Habitualmente el establecimiento de una LTV conllevará un procedimiento operacional, de tal manera que se evite afectar la operación de los trenes (por ejemplo la actuación del freno de emergencia porque se aplica una LTV muy cercana a la posición del tren).

Existen dos tipos de LTVs:

- LTVs estáticas o predefinidas.

- LTVs dinámicas.

Las LTVs predefinidas permiten establecer grandes áreas en los que las LTVs están vigentes, y 3 escalones de velocidad (por ejemplo: 80 km/h, 160 km/h y 230 km/h). Es la solución más básica en cuanto a gestión de LTVs ya que ofrece muy poca flexibilidad en cuestión de áreas de establecimiento y velocidad de paso, por lo que suelen penalizar la explotación.

Las LTVs dinámicas de Nivel 1 son lo más parecido a la gestión flexible que puede ofrecer un sistema como el Nivel 2. Permiten establecer áreas de LTV con una resolución de circuito de vía y una resolución habitual de velocidad de paso de 5 km/h. Este sistema permite establecer la LTV sólo en la zona afectada y a la velocidad de paso que realmente es necesaria.

El procedimiento a seguir para el establecimiento de una LTV, bien desde el Puesto Central de ERTMS (PCE), bien desde el Puesto Local de Operación PLO-R es el siguiente:

- El equipo de gestión de LTV GR recibe la petición de establecimiento de una LTV procedente del PCE o del PLO-R.

- El equipo de gestión de LTVs GR envía dicha información a los LEUs dentro de su área, y también se la envía a los GR adyacentes para que estos, en caso necesario, puedan enviar los datos correspondientes a la LTV a los LEUs de su área. Así los trenes que se aproximen a la zona en donde esté establecida la LTV la podrán recibir con suficiente antelación.

- El operador no recibe confirmación de que la LTV está aplicada hasta que realmente se recibe la información en los LEUs.

Las limitaciones temporales de velocidad se aplican a todos los trenes independientemente de su categoría. Cada limitación es independiente de las otras, por lo que puede existir superposición entre las mismas, aplicándose siempre la más restrictiva. Cada LTV tiene su propia identidad lo que permite su revocación posterior de forma

individual. Una LTV con el mismo identificador, reemplazará a una recibida previamente.

2.2.3.6 Información de gradiente

Las características de la información del gradiente (
Figura 2.12) son:

- Es responsabilidad del sistema de vía el enviar la información de gradiente al equipo embarcado en el tren.
- La información de gradiente será enviada en forma de perfil.
- El proceso de ingeniería de aplicación deberá determinar la forma de garantizar la seguridad en los criterios de discretización del perfil de gradientes.

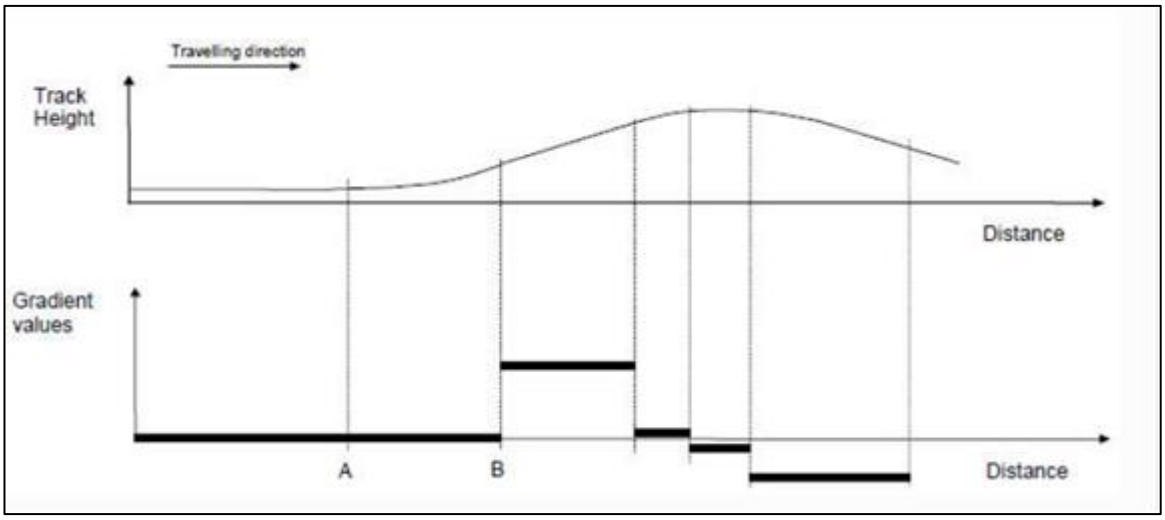


Figura 2.12. Discretización del perfil de gradientes

2.2.3.7 Perfil de Modo

El perfil de modo (paquete 80) se superpone a una autorización de movimiento para producir el cambio de modo desde FS, OS, SR, SB, PT, UN, SN o SE a uno de los dos modos siguientes (Ref. [3]):

1. OS (*On Sight*): Marcha a la vista
2. SH (*Shunting*): Maniobra

- También se puede definir el final del modo pero solamente para el caso de OS, ya que es el único para el que se define MA durante todo el área.

- La recepción de un nuevo MA sin perfil de modos provoca el borrado del perfil de modos actual.

- El comienzo de modo se establece con el *Max. Safe Front End*.

- El fin de modo se establece con el *Min. Safe Front End*.

El paquete 80 del perfil de modo contiene la información mostrada en la Tabla 2.2.

Variable	Descripción
V_MAMODE	Velocidad máxima permitida para el modo
D_MAMODE	Distancia al comienzo del área SH u OS.
M_MAMODE	Modo OS, SH
L_MAMODE	Longitud del área SH u OS
L_ACKMODE	Distancia para mostrar el reconocimiento del cambio de modo

Tabla 2.2. Información contenida dentro del paquete 80.

2.2.3.8 Track condition

La *Track Condition* es una funcionalidad permite informar al tren sobre condiciones de vía existentes a lo largo de la vía.

De todas las posibles condiciones de vía, las comúnmente utilizadas son las siguientes:

1. Zona neutra.
2. Túnel (implícita información de no parada).
3. Viaducto (implícita información de no parada).
4. Cierre de trampillas de aire acondicionado.
5. Parada no permitida.

Está permitida la superposición de informaciones incluso del mismo tipo. Es el equipo embarcado el encargado de gestionarlas.

2.2.3.9 Mensajes de texto

Es posible enviar textos predefinidos o textos libres, para ser mostrados en el DMI del tren. Ref. [3].

También es posible establecer condiciones de visualización tanto en distancia, modo, nivel, tiempo y reconocimiento por parte del maquinista.

Así mismo es posible establecer la prioridad del mensaje lo que condiciona la representación del mismo en el DMI.

2.2.3.10 Supervisión de velocidad

La supervisión de velocidad corresponde al equipo embarcado y consiste en determinar para cada momento la velocidad en función de la posición para respetar el MRSP y el EOA.

Comprenderá por lo tanto:

- La supervisión de la velocidad constante a mantener según el MRSP.
- Supervisión de la curva de frenado para alcanzar una velocidad inferior o nula.
- La velocidad de liberación.

Los distintos niveles de velocidad definidos en cada momento por el equipo embarcado son los siguientes:

- Velocidad permitida. Es la velocidad que el maquinista debe respetar en cada momento.
- Velocidad de alarma. Es la velocidad a partir de la cual se dispara una alarma al maquinista para indicar exceso de la misma. La alarma se mantiene hasta que la velocidad es igual o menor que la permitida.
- Velocidad de intervención de freno de servicio. Es la velocidad a partir de la cual se activa el freno de servicio si existe la interfaz correspondiente. Una vez que la velocidad es igual o inferior a la permitida, se libera el freno.
- Velocidad de intervención de freno de emergencia. Es la velocidad a partir de la cual se activa el freno de emergencia. Se utiliza para la supervisión de la velocidad de liberación, TRIP y respaldo del freno de servicio. Una vez activado el freno de servicio este se libera cuando el tren esté parado.

A continuación se describen los distintos escenarios de supervisión de velocidad posibles.

- Supervisión de velocidad constante.

  En este caso la velocidad permitida corresponde con el valor del MRSP. A partir de este valor se calcularán los valores de frenado de servicio y emergencia.

- Supervisión de curva de frenado.

  La supervisión de curva de frenado se puede dar por dos circunstancias:

1. Cuando el tren se aproxima a una velocidad objetivo inferior.

2. Cuando el tren se aproxima a un EOA.

El cálculo de la curva de frenado de servicio y emergencia deberán tener en cuenta las deceleraciones previstas para ambos tipos de frenados. La curva de emergencia se calcula teniendo por final el punto a proteger (DP) y considerando el *Max. Safe Front End*. La curva de frenado de servicio será la más restrictiva de las calculadas con la posición estimada sobre el EOA o con el *Max. Safe Front End* sobre el DP.

- Supervisión de velocidad de liberación.

La supervisión de la velocidad de liberación se aplica en la proximidad del EOA sobre un valor constante. La velocidad de liberación se puede gestionar a la hora de enviar la autorización de movimiento según los siguientes criterios:

1. Con un valor recibido junto con el MA.

2. Calculado por el equipo embarcado.

3. Usando un valor nacional.

El control de velocidad de liberación se activa en el momento en el que la velocidad de intervención del freno de servicio se iguala con dicho valor. Si se rebasa la velocidad de liberación se aplica automáticamente el freno de emergencia. También es calculado un límite inferior de velocidad de aviso.

2.2.3.11 Mando del sistema de freno

En caso de fallo del freno de servicio el freno de emergencia es activado:

- El freno de emergencia no es liberado hasta la parada del tren en los siguientes casos:

1. *TRIP*

2. Protección frente a movimiento contrario al sentido de marcha seleccionado en el tren.

3. Protección frente a movimiento contrario al sentido permitido por la autorización.

4. Protección frente a movimiento cuando la supervisión de tren parado está activada.

- Si el frenado de servicio se produce por error de enlace o inconsistencia de mensaje, este no se libera hasta la parada del tren. Una vez parado, el MA se recorta hasta la posición de la cabeza del tren. Se reanudará la marcha es SR, cambiando a FS al pasar por encima de una baliza ERTMS.

2.2.3.12 Valores Nacionales

Los valores nacionales definen los parámetros relativos a determinadas variables que son de aplicación en una línea o líneas determinadas (valor del NID_COUNTRY).

Si los valores no han sido recibidos por la eurocabina, esta aplicará los valores por defecto.

Deben quedar memorizados a bordo incluso cuando la eurocabina está aislada y sin energía. Ref. [3]

2.2.4 Modos de funcionamiento

A continuación se describen los modos de funcionamiento previstos en la especificación SRS. Ref. [3].

Los modos posibles son los siguientes:

- *Full supervisión* (FS). Supervisión total.

  El equipo embarcado tiene la información de autorización de movimiento y la información de vía (gradiente y SSP) para la supervisión total. Este modo no puede ser seleccionado por el maquinista, el equipo embarcado es responsable de la supervisión del tren. El maquinista es responsable de la conducción del tren dentro de los parámetros de velocidad y autorización determinados por el equipo embarcado.

- *On Sight* (OS). Marcha a la vista.

  En este modo se permite al tren entrar en un circuito de vía ocupado. El cambio a este modo tiene que ser enviado desde el equipamiento de suelo. El equipo embarcado es responsable de la supervisión del movimiento del tren y control de la velocidad definida para el modo OS. El maquinista es responsable de verificar de forma visual la ocupación de la vía sobre la que circula.

- *Staff Responsible* (SR). Responsabilidad del maquinista.

  Es utilizado cuando no hay información de la ruta, por ejemplo:

1. Después del arranque de la eurocabina.

2. Al realizar un rebase de señal (OVERRIDE).

3. Después de un fallo del sistema de vía.

En este modo el equipo embarcado supervisa la velocidad establecida para este modo. El maquinista debe respetar la señalización lateral existente y en su defecto supervisar que la vía está libre y las agujas en posición, siguiendo en cada caso el procedimiento degradado establecido.

- *Shunting* (SH). Maniobra.

  El equipo embarcado supervisa la velocidad establecida para este modo y el no sobrepasar ninguna baliza con información restrictiva para este modo.

  Una vez pasado a modo SH se considera fin de misión. Este modo puede ser seleccionado por el maquinista a tren parado o bien enviado desde el equipo de vía mediante una orden de cambio de modo.

- *Unfitted* (UN). Sin equipamiento.

  Este modo de operación será utilizado en zonas no equipadas. El equipo embarcado supervisará la velocidad determinada para este modo. El maquinista debe respetar la señalización lateral y los procedimientos operacionales previstos.

- *Sleeping* (SL). Modo de funcionamiento de una eurocabina esclava. Modo de funcionamiento exclusivamente relacionado con el equipo embarcado.

- *Stand By* (SB). Modo inicial de la eurocabina una vez arrancada. Modo de funcionamiento exclusivamente relacionado con el equipo embarcado.

- *Trip* (TR). Modo especial que provoca el frenado de emergencia ante un evento considerado peligroso.

  Una vez que el tren ha parado, se pedirá reconocimiento al maquinista para salir de este modo.

- *Post Trip* (PT). Modo al que pasa la eurocabina después del reconocimiento por parte del maquinista de un TRIP.

Una vez en este modo, se produce la liberación del freno de emergencia. Para avanzar el maquinista tendrá que elegir entre comenzar misión de nuevo (con paso a SR) o paso a modo SH.

- *System Failure* (SF). Modo de fallo de la eurocabina. Modo de funcionamiento exclusivamente relacionado con el equipo embarcado.

- *Isolation* (IS). Modo de aislamiento de la eurocabina. Modo de funcionamiento exclusivamente relacionado con el equipo embarcado.

- *No Power* (NP). Estado sin alimentación en la eurocabina. Modo de funcionamiento exclusivamente relacionado con el equipo.

- *Non Leading* (NL). Modo de funcionamiento para una eurocabina presente en un puesto de conducción esclavo sin conexión a la cabina de conducción principal. Modo de funcionamiento exclusivamente relacionado con el equipo embarcado.

- *Reversing* (RV). Modo de funcionamiento que permite al maquinista el cambio de sentido de la marcha.

2.2.5 Transiciones de nivel

Hay que considerar dos tipos de transiciones de nivel: Las producidas de forma degradada por fallo del sistema y las programadas.

Las primeras se producen por un fallo del sistema y afectan exclusivamente al equipo embarcado.

Dentro del grupo de las transiciones programadas tendremos dos tipos fundamentales:

- Las de entrada y salida de la línea equipada.

Esta transición se produce a nivel 0. Previamente a la transición se envía desde suelo el paquete correspondiente con el anuncio del punto en el que se realizará la misma.

En el punto de transición se enviará desde suelo el paquete con la orden de ejecución de la transición.

El resto de requerimientos para la transición son exclusivos del equipamiento embarcado.

- Las de comienzo de misión en el interior de la línea.

  Las transiciones previstas dentro de la línea se realizarán enviando en el paquete correspondiente los niveles disponibles. El equipo embarcado elegirá aquel de mayor prioridad que encuentre disponible.

  A tren parado el maquinista podrá seleccionar el nivel en el comienzo de misión.

2.2.6 Lenguaje ERTMS N1

Cada telegrama contenido en una eurobaliza que forma un mensaje de un grupo de eurobalizas está formado por una cabecera y una serie de paquetes. Ref. [3].

El telegrama debe terminar con el paquete de fin (paq. 255).

El comportamiento del sistema debe ser independiente del orden en el que estén los paquetes dentro del telegrama, con excepción del paquete que determina la información infill (paq. 136) que debe estar colocado antes de los paquetes que contienen dicha información.

No está permitido dentro de un mismo mensaje la repetición del mismo paquete válido para la misma dirección, con excepción del paquete 44 (Aplicaciones externas), paquete 65 (LTV) y paquete 66 (revocación de LTV).

A continuación, se describen los elementos básicos del lenguaje ERTMS.

2.2.6.1 Variables

La variable es la unidad atómica de información con significado.

Las variables están tipificadas, de acuerdo con un significado. Pueden tener valores especiales asociadas al tipo de la variable. Los nombres de las variables son únicos.

Las variables tienen un prefijo que hace referencia a su tipo:

A_ Aceleración
NC_ Número de clase
D_ Distancia
NID_ Identificador
G_ Gradiente
Q_ Modificador
L_ Longitud
T_ Tiempo/Fecha
M_ Miscelánea
V_ Velocidad
N_ Número
X_ Texto

2.2.6.2 Paquetes

Los paquetes son un conjunto de variables agrupadas con una estructura definida.

Dicha estructura consiste en una cabecera del paquete. La Tabla 2.3 muestra la información en la cabecera del paquete.

NID_ PACKET	Identificador del paquete
Q_DIR	Indica el sentido de marcha para el que la información es válida
L_PACKET	Número de bits en el paquete
Q_SCALE	Parámetro que indica la escala para las distancias
…	Conjunto de variables definido de acuerdo al paquete concreto

Tabla 2.3. Información contenida en la cabecera del paquete.

2.2.6.3 Telegramas

Un telegrama es la información transmitida por una baliza dentro de un grupo. Está compuesto por una cabecera y una serie de paquetes. Un telegrama termina con el paquete 255 “Fin de Información”.

2.2.6.4 Mensajes

Un mensaje es la información transmitida por un grupo de balizas.

Cada baliza del grupo transmite un telegrama. La secuencia de telegramas en el mensaje es ordenada por el número de baliza en el grupo. El comportamiento del receptor no debe depender de la secuencia de transmisión de los paquetes Excepto para la información Infill.

2.2.7 ETCS subsistema de equipo embarcado

El esquema básico de los componentes del equipo embarcado se muestra en la Figura 2.13.

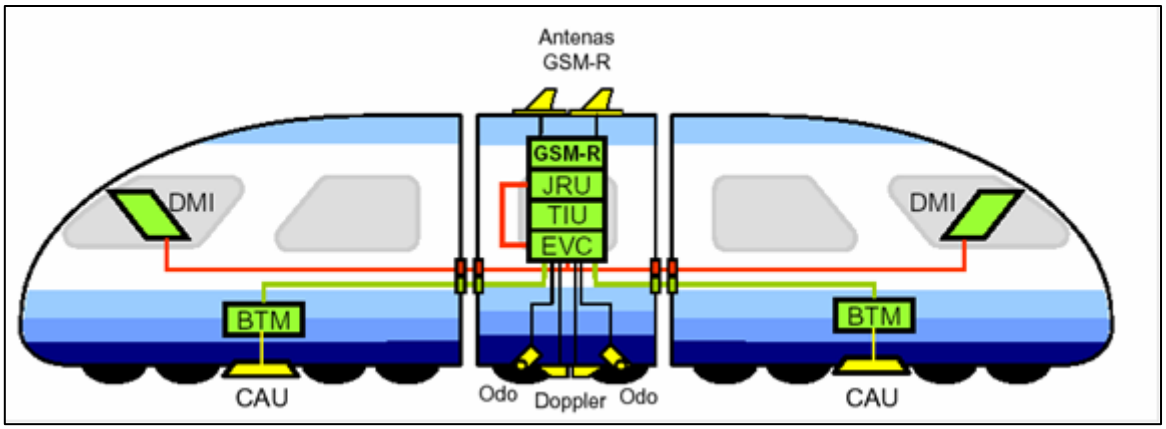


Figura 2.13. Arquitectura tipo de equipo embarcado en tren

A continuación, se describen los componentes que forman el equipo embarcado del sistema ETCS.

2.2.7.1 EVC. *European Vital Computer*

El EVC (*European Vital Computer*) es el núcleo del equipo embarcado, calcula las curvas de frenado y los perfiles de velocidad. Sus funciones principales son:

- Controla la velocidad permitida.
- Recibe los mensajes del subsistema lado vía.
- Conoce los datos específicos del tren y sus características de frenado.
- Controla las actividades de frenado.

2.2.7.2 Odómetros

Los odómetros son elementos de medición que permiten calcular principalmente la velocidad a la que circula el tren y la distancia recorrida por el mismo.

Existen dos tipos de odómetros utilizados en el ámbito ferroviario: El odómetro Tacogenerador y el odómetro con sensor Radar Doppler.

- Odómetro Tacogenerador.

  El odómetro tacogenerador cuenta pulsos por vuelta y es capaz de trasmitir información al EVC:

  1. La distancia recorrida por el tren.
  2. La rotación de las ruedas y dirección de la marcha.

3. La velocidad del tren.

4. La aceleración del tren.

- Odómetro con sensor Radar Doppler.

  El odómetro con sensor Radar Doppler es capaz de realizar mediciones de velocidad y distancia con una alta precisión.

  Además, su medición no se ve afectada en caso de deslizamiento como podría ocurrir con un odómetro tacogenerador.

2.2.7.3 DMI: *Driver Machine Interface*

El DMI (driver machine interface) es la pantalla que tiene el maquinista en su puesto de conducción (Figura 2.14). Sus funciones principales son:

- Entrada de información por parte del conductor.

- Presentación de información al conductor.

- Recoger las acciones de respuesta por parte del conductor (selección de modo, confirmación, reconocimiento, etc.).

Figura 2.14. Ejemplo de DMI

2.2.7.4 JRU: *Juridical Recorder Unit*

El JRU (*juridical Recorder Unit*) es un elemento que se encarga de registrar los datos del movimiento del tren. Estos datos son tanto los telegramas transmitidos por las Eurobalizas, como las acciones de operación realizadas por el maquinista.

Además, otra de sus funciones es la de proporcionar pruebas objetivas sobre las causas de los posibles accidente.

2.2.7.5 Antena tren lectora Eurobaliza

La antena lectora de Eurobalizas es una antena situada en la parte inferior del tren. Cuando el tren pasa por encima de una baliza, esta antena es la encargada de interactuar con la baliza.

Las principales funciones de la antena lectora son:

- Emitir una señal de activación a 27,095 MHz.
- Activar la Eurobaliza por acoplamiento inductivo.
- Recibir datos transmitidos desde la Eurobaliza de forma intermitente.

3.Normativa CENELEC EN-50126 e Ingeniería RAMS

3.1 Introducción a CENELEC

El Comité Europeo de Normalización (CEN) desarrolla trabajos de Normalización que cubren todos los sectores técnicos con excepción del campo electrotécnico, que es competencia del Comité Europeo de Normalización Electrotécnica (CENELEC).

CELENEC fue creada en 1973 en Bélgica.

El papel de esta organización, sin ánimo de lucro, es crear normas europeas que fomenten la competitividad de la industria europea a nivel mundial y ayuden a crear el mercado interior europeo.

Para realizar esta actividad, este organismo fomenta la adopción de normas ISO.

3.2 Objetivos de las normas CENELEC

Las normas CENELEC definen las condiciones para el acceso de los bienes y servicios electrotécnicos al mercado europeo con el máximo consenso posible basado en la solución más universal y en el menor tiempo posible.

Los objetivos básicos de CENELEC son los siguientes:

- Preparar nuevas normas Europeas o documentos de armonización sobre aquellos temas en los que no existen normas Internacionales o Nacionales.

- Promover la implantación en Europa de las normas desarrolladas por ISO.

3.3 Áreas de actuación de las normas CENELEC

A continuación se listan algunos de los ámbitos en los que CENELEC ha elaborado normas Ref. [10]:

- Autobuses radiales.
- Sistemas electrónicos para el transporte de superficie.
- Sistemas de comunicación, señales y procesamiento ferroviarios.
- Sistemas electrónicos para hogares y edificios.
- Cables para comunicaciones.
- Sistemas de datos vía radio.
- Sistemas de distribución cableada para TV y señales acústicas.
- Equipos receptores de emisiones.
- Informática médica.
- Productos EMC para las tecnologías de la información.
- Aplicaciones de refrigeración de infrarrojos.
- Sistemas de alarma.
- Aspectos electrotécnicos de los equipos de telecomunicación.
- Seguridad y eficiencia eléctrica en equipos de tecnologías de la información y las telecomunicaciones.
- Automatización del diseño electrónico.
- Telecontrol.
- Lectura remota de medidores.
- interconexión de los equipos de tecnología de la información.
- Sistemas de microprocesamiento.
- Normas para terminales de multimedia.
- Instalaciones para el control del tráfico aéreo.
- Equipos espaciales y aplicaciones específicas de la tecnología espacial.
- Componentes activos electrónicos utilizados en los equipos de tecnologías de la información.

Dentro de todos estos ámbitos, el presente proyecto se va a centrar en el ámbito de sistemas de comunicación, señales y procesamiento ferroviario.

3.4 Normativas utilizadas en el ámbito ferroviario

Existe un amplio número de normas redactadas por CENELEC referentes al ámbito ferroviario. A continuación se listan las más habituales Ref. [10]:

- Cenelec EN 50119: Aplicaciones ferroviarias - Instalaciones fijas - Tracción eléctrica - Líneas aéreas de contacto

- Cenelec EN 50121: Aplicaciones ferroviarias - Compatibilidad electro-magnética

- Cenelec EN 50122: Aplicaciones ferroviarias - Instalaciones fijas

- Cenelec EN 50124: Aplicaciones ferroviarias - Coordinación de aislamiento

- Cenelec EN 50125: Aplicaciones ferroviarias - Condiciones ambientales para el equipo.

- Cenelec EN 50126: Aplicaciones ferroviarias – Especificación y demonstración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS).

- Cenelec EN 50128: Aplicaciones ferroviarias – Sistemas de comunicación, señalización y procesamiento. Software para sistemas de control y protección del ferrocarril.

- Cenelec EN 50129: aplicaciones ferroviarias - Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización.

- Cenelec EN 50159-1:2001 Aplicaciones ferroviarias - Sistemas de comunicación, de señalización y de procesado.

Este proyecto va a centrar la atención en la norma EN-50126 Ref. [1] . En el apartado siguiente se describe dicha norma.

3.5 Norma EN-50126

3.5.1 Introducción

La norma EN-50126 Ref. [1] promueve la cooperación entre la autoridad Ferroviaria y la industria ferroviaria, con una gran variedad de estrategias para alcanzar una óptima combinación de la RAMS y los costes en las aplicaciones ferroviarias.

La RAMS en el ámbito ferroviario describe el nivel de confianza de un sistema que nos permite asegurar que se alcanzará este objetivo.

La RAMS de un sistema se puede caracterizar como un indicador cuantitativo y cualitativo del grado en el que el sistema y componentes que lo integran, puede funcionar según lo especificado, siendo disponible y seguro.

RAMS es una característica de los sistemas de operación a largo plazo y se alcanza por la aplicación de conceptos de ingeniería establecidos, métodos y herramientas y técnicas a lo largo del ciclo de vida del sistema.

3.5.2 Objeto y campo de aplicación

Esta norma está orientada específicamente al sector ferroviario y tiene como objetivos principales:

- Definir la RAMS en términos de Fiabilidad, Disponibilidad, Mantenibilidad y Seguridad y sus relaciones.

- Permitir controlar y gestionar de manera efectiva los conflictos existentes entre los elementos RAMS.

- Definir un proceso basado en el ciclo de vida del sistema y las tareas asociadas al mismo, para la gestión de la RAMS.

- Definir un proceso sistemático para especificar los requisitos RAMS y demostrar que son alcanzados.

La presente norma es aplicable a la especificación y demostración de la RAMS para sistemas ferroviarios, junto a todos los subsistemas y componentes que forman los sistemas complejos. Específicamente:

- Sistemas nuevos.
- Integraciones de sistemas nuevos en sistemas ya existentes.
- Modificaciones en sistemas puestos en operación anteriormente a este estándar.
- Todas las fases relevantes del ciclo de vida de una aplicación.

3.5.3 RAMS ferroviario y calidad del servicio

El objetivo final de los sistemas ferroviarios es el de alcanzar un tráfico determinado en un tiempo determinado y "de manera segura". Una característica muy importante de este objetivo es la calidad del servicio que se proporciona.

El RAMS ferroviario describe el nivel de confianza con la que un sistema puede garantizar el alcance de los objetivos para los que ha sido diseñado, por lo tanto, tiene una clara influencia en la calidad del servicio que se le proporciona al usuario.

Por lo tanto, la calidad del servicio se basa en el RAMS ferroviario junto con otros atributos como costes, frecuencia del servicio o funcionalidad.

3.5.3.1 Elementos del RAMS ferroviario

Los elementos a los que se refriere al hablar de la RAMS son: Fiabilidad, Disponibilidad, Mantenibilidad y Seguridad.

Aunque en nuestro caso, en lugar del término seguridad, utilizaremos el término *Safety*. De esta manera se puede diferenciar la acepción del término seguridad en relación a la resistencia al vandalismo y comportamientos humanos no razonables. Esta acepción no entra dentro del objetivo de esta norma y es por ello que en el presente proyecto se utiliza el término Safety.

Safety y Disponibilidad están relacionados en el sentido de que una debilidad en uno de ellos o una mala gestión de los conflictos entre los requisitos de disponibilidad y seguridad, puede impedir el alcanzar un sistema fiable.

Los objetivos de Safety y Disponibilidad, sólo pueden ser alcanzados mediante un control continuo de los requisitos de Fiabilidad y Mantenibilidad así como la realización de las actividades de operación y mantenimiento en el entorno del sistema.

La Figura 3.1 muestra la interrelación de los elementos de la RAMS ferroviaria.

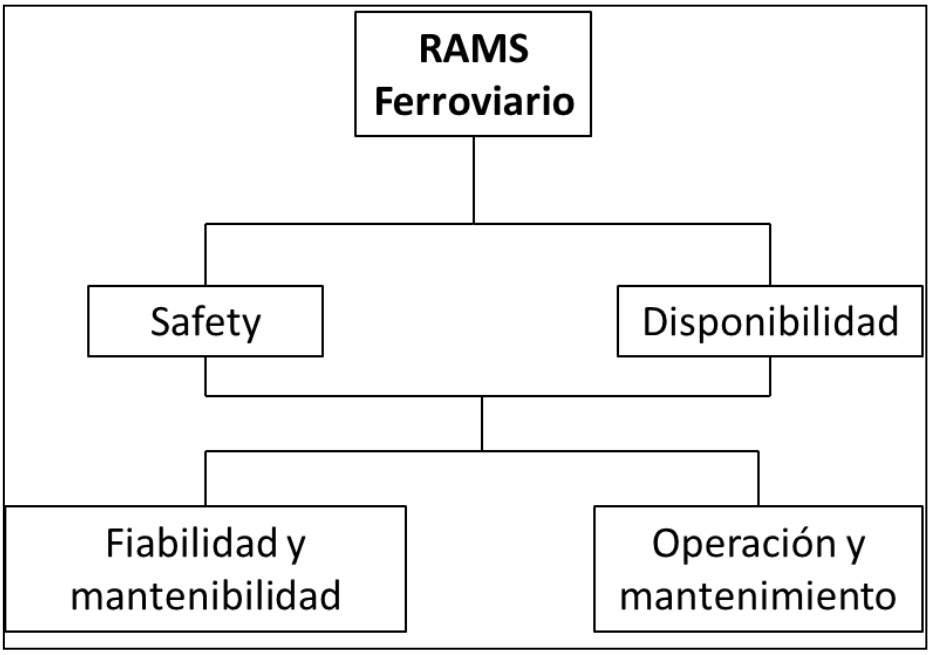


Figura 3.1. Interrelación de los elementos de la RAMS Ferroviaria.

Los conceptos técnicos de Disponibilidad se basan en el conocimiento de:

Fiabilidad:

- Todos los posibles modos de fallo en la aplicación específica y entorno.
- La probabilidad de que ocurra cada fallo o alternativamente, ratio de ocurrencia de cada uno.
- El efecto de un fallo en la funcionalidad del sistema.

Mantenibilidad:

- Tiempo para llevar a cabo el mantenimiento planeado.
- Tiempo para la detección, identificación y localización de fallos.
- Tiempo para restablecer un sistema ante un fallo.

Operación y mantenimiento:

- Todos los modos de operación y mantenimiento requeridos durante todo el ciclo de vida del sistema.
- Cuestiones debidas al factor humano.

Los conceptos técnicos de *Safety* se basan en el conocimiento de:

- Todos los posibles peligros que pueden darse en el sistema, en todos los modos de operación y ambientes.

- Las características de cada peligro en términos de la gravedad de las consecuencias.

- Todos los modos de fallo de un sistema que pueden llevar a un peligro.

- Probabilidad de ocurrencia de cada evento, fallo, modo de fallos, condiciones de ambiente en la aplicación.

- La mantenibilidad de las partes del sistema relacionadas con la seguridad en lo referente a la facilidad de llevar a cabo el mantenimiento del sistema, la probabilidad de que se produzcan errores en el sistema y el tiempo necesario para devolver el sistema a un estado de seguridad.

- La operación y el mantenimiento del sistema de las partes del mismo relacionadas con la seguridad en lo referente a la influencia de factores humanos sobre el mantenimiento del sistema, las herramientas, instalaciones y procedimientos utilizados durante el mantenimiento y los controles y medidas tomadas para enfrentarse a un peligro y mitigar sus consecuencias.

3.5.3.2 Factores que influyen en la RAMS Ferroviaria

Existen tres vías posibles que pueden influir en la RAMS del sistema, que son: fuentes de fallos debidos a condiciones del sistema, fuentes de fallos debidos a condiciones de operación y fuentes de fallos debidos a condiciones de mantenimiento. Estas fuentes de fallos además pueden interactuar.

Para la realización de sistemas fiables, es necesario identificar los factores que pueden influir en la RAMS del sistema, y evaluar sus efectos mediante la aplicación de los controles apropiados para la optimización del funcionamiento del sistema.

Un grupo importante de factores a tener en cuenta son los factores humanos.

Se pueden clasificar todos los factores en dos grupos, *Factores específicos de Ferroviario* y *Factores Humanos*, estos últimos pueden ser definidos como el impacto que las características, expectativas y comportamiento humano tienen sobre los sistemas.

Cómo mínimo cada uno de estos grupos ha de incluir:

- Factores específicos de Ferroviario:
  - Operación del sistema.
  - Condiciones de Entorno.
  - Condiciones de aplicación.
  - Condiciones de operación.
  - Categorías de fallos.

- Factores Humanos:
  - El reparto de funciones humano vs máquina.
  - El funcionamiento humano dentro del sistema.
  - Requerimientos del sistema debidos a comportamiento, motivación, tiempo de reacción, etc.
  - Requerimientos del sistema debidos a capacidad de procesado de información.
  - Efectos por factores de interface humano/máquina.
  - Factores humanos en el diseño y desarrollo del sistema.

3.5.3.3 Significado de alcanzar los requisitos RAMS

Cuando se alcanzan los requisitos RAMS se obtiene:

- Un control efectivo de los factores que influyen en la RAMS, lo que se obtiene poniendo en marcha los mecanismos y procedimientos contra errores. Para ello es necesario tener en cuenta tanto los fallos sistemáticos como los aleatorios.

- Precaución en minimizar las posibilidades de daño. La precaución es una combinación de: Prevención (minimizar la probabilidad de daño) + Protección (minimizar las consecuencias de un daño).

3.5.3.4 Especificación de los requisitos RAMS

De acuerdo a la norma EN-50126 Ref. [1], la estructura básica y contenidos de las especificaciones RAMS ha de ser:

1. Identificación del proyecto:

   I. Identificar proyecto, Entregables, Fechas.
   II. Organización del proyecto y operación.

2. Descripción General del sistema:

   I. Descripción técnica.
   II. Aplicación y operación específicas.
   III. Descripción técnica de los subsistemas.

3. Condiciones de Operación y mantenimiento:

   I. Identificar los modos de operación.
   II. Esperanza de vida.
   III. Condiciones ambientales.

4. Fiabilidad:

   I. Objetivos de fiabilidad, particularizar según la aplicación específica.
   II. Modos de fallo del sistema y *Mean Time Between Failure* (MTBF).
   III. Efecto Operación/Rendimiento.

5. Mantenimiento y reparación:

   I. Mantenimiento preventivo.
   II. Reparación.

6. Seguridad:

   I. Objetivos de seguridad.
   II. Condiciones de peligro.
   III. Funciones relacionadas con la seguridad y Fallos.

7. Disponibilidad:

   I. Especificaciones de disponibilidad.

8. Demostración de la ejecución RAMS:

   I. Gestión y organización RAMS.
   II. Disponibilidad de recursos RAMS.
   III. Planes y programas RAMS.
   IV. Revisión de informes relacionados con RAMS.
   V. Análisis de Informes RAMS.
   VI. Resultados de testeo RAMS (de componentes).
   VII. Estadísticas de Fallos en adquisición de datos.
   VIII. *Safety Case* de aplicación específica.
   IX. Validación y aceptación de sistemas.

X. Monitorización de la ejecución RAMS en la fase de operación temprana.
XI. Evaluación del coste del ciclo de vida.

9. Programa RAMS.

3.5.3.5 Riesgos

El concepto riesgo consiste en una combinación de dos elementos:

1. Probabilidad de que ocurra uno o varios eventos que conduzcan a un peligro o la Frecuencia de dichas ocurrencias.

2. Consecuencia derivada de dicho peligro.

3.5.3.5.1 Análisis de riesgos

El análisis de riesgos se debe de llevar a cabo en varias fases del ciclo de vida del sistema por la autoridad responsable de esa fase, además ha de ser documentada. Dicha documentación ha de contener:

1. Metodología de análisis.

2. Presuposiciones, limitaciones y justificaciones de dicha metodología.

3. Resultado de la identificación de peligros.

4. Estimación de los resultados de riesgos y sus niveles de confianza.

5. Fuentes y niveles de confianza de los datos.

6. Referencias.

El número de categorías y la escala a aplicar deben ser definidas por la autoridad Ferroviaria de manera apropiada para la aplicación que se está considerando.

La Tabla 3.1 muestra las categorías típicas de la probabilidad o de la frecuencia con que se da un suceso de peligro.

Categoría	Descripción
Frecuente	Es posible que ocurra frecuentemente. La amenaza se reproducirá continuamente.
Probable	Ocurrirá varias veces. Se puede esperar que la amenaza ocurra a menudo.
Ocasional	Es posible que ocurra varias veces. Se puede esperar que la amenaza ocurra varias veces.
Remota	Es posible que ocurra alguna vez durante el ciclo de vida del sistema. Se puede suponer razonablemente que la amenaza se va a producir.
Improbable	Poca probabilidad pero posible. Se puede asumir que la amenaza puede ocurrir excepcionalmente.
Increíble	Extremadamente poco probable. Se puede asumir que la amenaza no ocurrirá.

Tabla 3.1 Frecuencia con que se dan Sucesos de Peligro

El análisis de consecuencias se debe utilizar para calcular el impacto probable. La Tabla 3.2 muestra los niveles típicos de gravedad de los peligros y las consecuencias asociadas a cada nivel de gravedad.

Nivel de severidad	Consecuencias para las personas o el medio natural	Consecuencias para el servicio
Catastrófico	Varias víctimas mortales y/o múltiples heridos graves y daño grave al medio natural	-
Crítico	Una víctima mortal y/o herido grave y/o daños significativos al medio natural	Pérdida de un sistema principal
Marginal	Herido leve y/o amenaza significativa para el medio natural	Daño grave de uno o varios sistemas
Insignificante	Posible herido leve	Daño leve de un sistema

Tabla 3.2 Niveles de gravedad del peligro.

3.5.3.5.2 Evaluación y aceptación de riesgos

La evaluación de riesgos se debe realizar combinando la frecuencia con que ocurre un suceso peligroso con la gravedad de sus consecuencias, con el fin de establecer el nivel de riesgo generado por el suceso amenazante. La Tabla 3.3 muestra una matriz de "frecuencia-consecuencia".

Frecuencia de Ocurrencia	Niveles de Riesgo			
Frecuente				
Probable				
Ocasional				
Remota				
Improbable				
Increíble				
	Insignificante	Marginal	Crítico	Catastrófico
	Niveles de gravedad de la consecuencia de la amenaza			

Tabla 3.3. Matriz Frecuencia -Consecuencia

Para llevar a cabo la aceptación de riesgos, es necesario basarse en un principio generalmente aceptado. Algunos ejemplos de aceptación son:

- Tan Reducido Como Razonablemente Viable (ALARP)
- *Globalement Au Moins Aussi Bon* (GAMAB)
- Mortalidad Endógena Mínima (MEM)

La Tabla 3.4 define las categorías cualitativas de riesgo así como las acciones que deben tomarse ante cada categoría.

Categoría de Riesgo	Acciones que se han de tomar ante cada categoría
Intolerable	Debe eliminarse.
No Deseable	Sólo debe aceptarse cuando la reducción del riesgo sea impracticable y con el acuerdo de la Autoridad Ferroviaria.
Tolerable	Aceptable con un control adecuado y con el acuerdo de la Autoridad Ferroviaria.
Insignificante	Aceptable con/sin el acuerdo de la Autoridad Ferroviaria.

Tabla 3.4. Categorías Cualitativas de Riesgos.

Una vez que se tiene una definición cualitativa de los riesgos, se puede cumplimentar la matriz Frecuencia – Consecuencia (Tabla 3.3), de tal manera que se obtiene una matriz de evaluación y aceptación de riesgos. Un ejemplo de matriz es la mostrada en la Tabla 3.5.

Frecuencia de Ocurrencia	Niveles de Riesgo			
Frecuente	No deseable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	No deseable	Intolerable	Intolerable
Ocasional	Tolerable	No deseable	No deseable	Intolerable
Remota	Despreciable	Tolerable	No deseable	No deseable
Improbable	Despreciable	Despreciable	Tolerable	Tolerable
Increíble	Despreciable	Despreciable	Despreciable	Despreciable
	Insignificante	Marginal	Crítico	Catastrófico
	Niveles de gravedad de la consecuencia de la amenaza			

Tabla 3.5. Ejemplo típico de Evaluación y Aceptación de Riesgos.

3.5.3.5.3 Integridad en la seguridad

La integridad en la seguridad puede verse como una combinación de elementos cuantificables (por ejemplo fallos aleatorios en el HW) y no cuantificables (fallos en documentación, especificación, procesos, etc.). La reducción de riesgos externos junto con la reducción de riesgos del sistema, permiten alcanzar la reducción de riesgos necesaria para que el sistema pueda alcanzar su nivel de seguridad objetivo.

Los sistemas con mayores requisitos de integridad son, con mayor probabilidad, más caros de realizar.

Los requisitos de seguridad de cada sistema definen el nivel de integridad para su implementación. Durante el diseño, los niveles de seguridad proporcionan un mecanismo para la distribución de los requisitos de seguridad a los componentes de la arquitectura del sistema. A la hora de la implementación, cada nivel de integridad define una combinación de técnicas para el desarrollo del sistema que proporcionan la confianza de que se alcance el nivel de seguridad apropiado.

3.5.4 Gestión RAMS

La gestión RAMS es un proceso de gestión que permite controlar los factores RAMS en aplicaciones específicas ferroviarias. Este proceso de gestión se basa en el cumplimiento de un ciclo de vida. Este proceso incluye:

- Definición de los requisitos RAMS.
- Valoración y control de las amenazas a la RAMS.
- Planificación e implementación de las tareas RAMS.
- Alcanzar el cumplimiento de los requisitos RAMS.
- Monitorización durante el ciclo de vida del cumplimiento.

El riesgo de seguridad tolerable de un sistema Ferroviario, para cualquier Autoridad Ferroviaria, depende del criterio de seguridad fijado por la Autoridad Nacional Reguladora de Seguridad o por la Autoridad Ferroviaria de acuerdo con la Autoridad Reguladora de Seguridad.

3.5.4.1 Ciclo de vida del sistema

El ciclo de vida del sistema es una secuencia de fases, cada una de las cuales contiene tareas, que cubren toda la vida del sistema, desde el concepto inicial, hasta la retirada del servicio y su eliminación. El ciclo de vida proporciona la estructura ideal para la planificación, gestión, control y monitorización de todos los aspectos de un sistema, incluida la RAMS.

La Figura 3.2 muestra la secuencia de fases definida en la norma UNE-50126 Ref. [1].

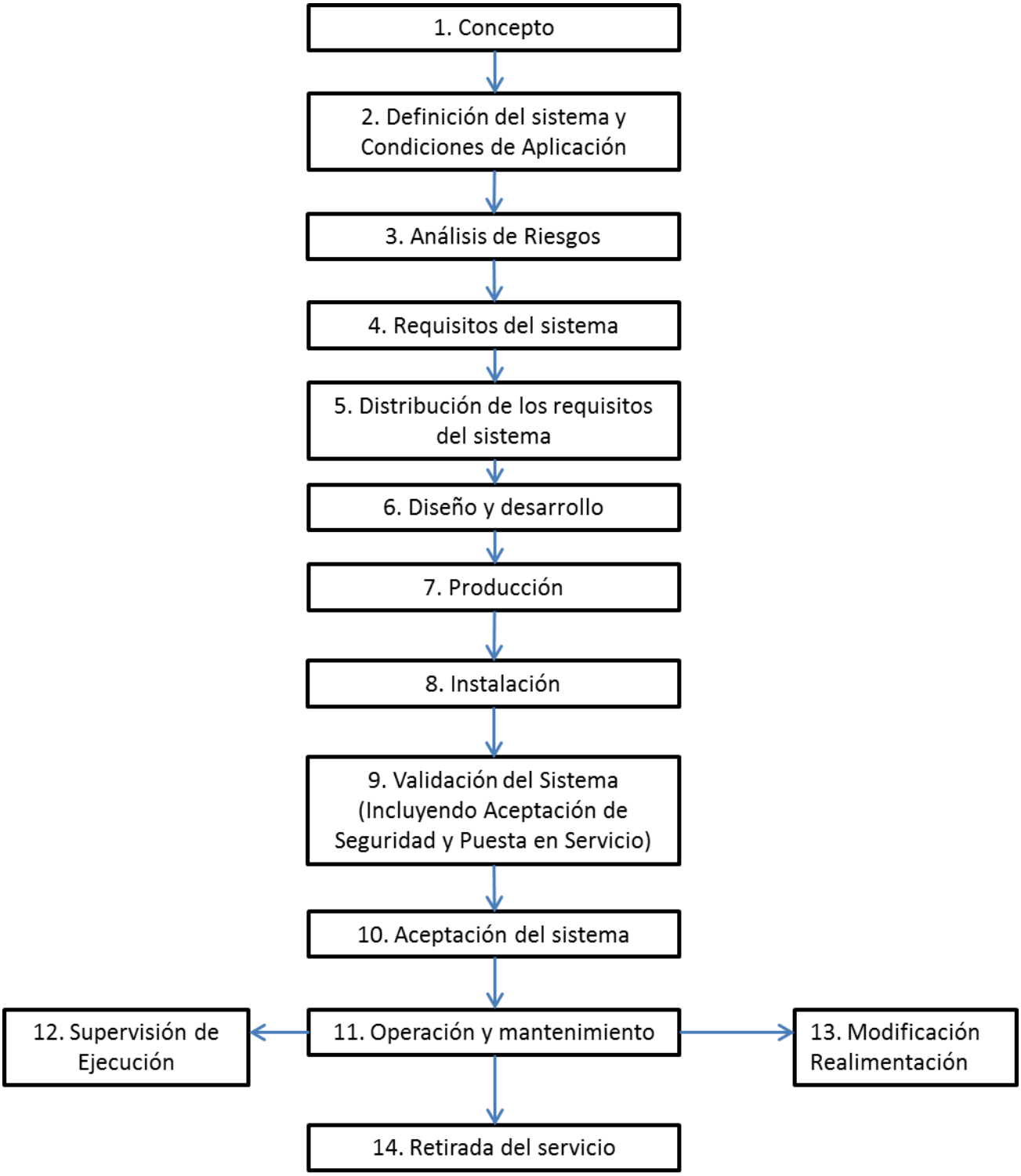


Figura 3.2. Ciclo de Vida del Sistema

El proceso de desarrollo se termina con la instalación, y el proceso de seguridad asociado con la finalización y envío del caso de seguridad a la autoridad ferroviaria para su validación.

El objetivo de la verificación es demostrar que para entradas específicas, los entregables de cada fase coinciden plenamente con los requisitos de esa fase.

El objetivo de la validación es demostrar que el sistema que se está considerando, en cada paso de su desarrollo y después de su instalación, cumple los requisitos en todos los aspectos.

El proceso de seguridad genera tres documentos entregables importantes:

- **Plan de Seguridad.** Contiene los detalles de los procesos de análisis y valoración de seguridad, así como de la estructura organizativa dispuesta para implementar estos procesos. El Plan de Seguridad conduce los procedimientos del proceso de seguridad.

- ***Hazard Log***. Contiene una lista de los sucesos peligrosos y detalla las medidas utilizadas para reducir los riesgos asociados con cada peligro. El Seguimiento de peligros conduce los aspectos técnicos del proceso de seguridad.

- ***Safety Case***. Integra la evidencia técnica y de procedimientos necesaria para la validación/certificación.

A lo largo del próximo capítulo se va a desarrollar con más profundidad cada fase del ciclo de vida definido en la norma EN-50126 Ref. [1], y se ampliará la definición de los documentos anteriormente nombrados así como los de muchos más no tan básicos en el proceso de seguridad pero también necesarios.

4. Ciclo de vida del sistema para el proceso de Seguridad en ERTMS N1

4.1 Introducción

En este capítulo, se va a seguir el ciclo de vida descrito en el apartado 3.5.4.1 del presente proyecto desde el punto de vista del proceso de seguridad. Para cada fase se estudiarán los objetivos a alcanzar definidos por la norma EN-50126 Ref. [1] así como la documentación, tanto de entrada como a generar por parte del equipo de seguridad, necesaria.

Al tratarse del proceso de seguridad, no todas las fases van a ser de aplicación. Por lo tanto, el ciclo de vida mostrado en el capítulo anterior se va a ver modificado y algunas de sus fases no van a aparecer.

De esta manera, el ciclo de vida quedaría como se muestra en la Figura 4.1.

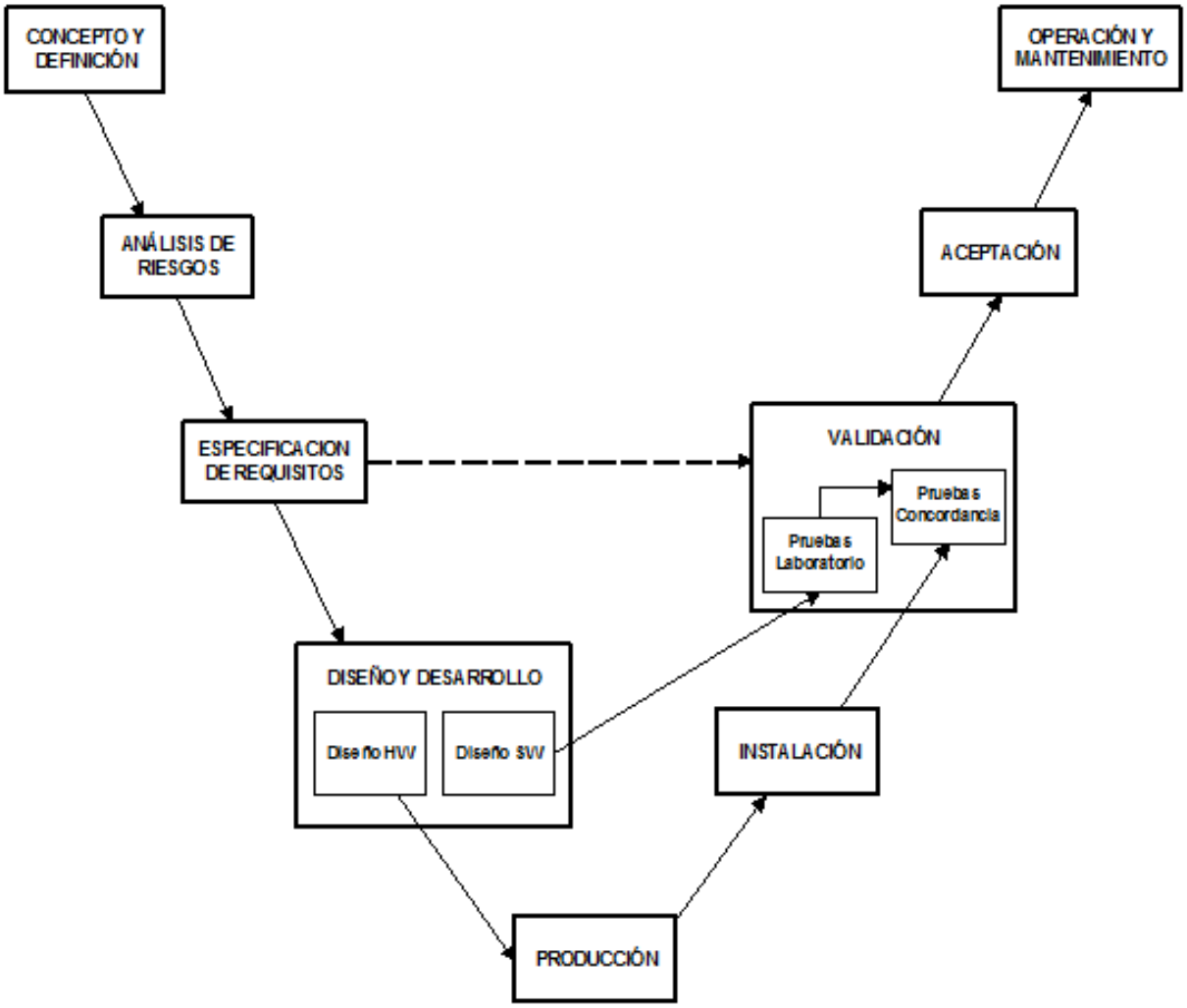


Figura 4.1. Ciclo de vida en V para el proceso de Seguridad.

Para cada fase se van a enumerar los objetivos a alcanzar en dicha fase de acuerdo a la norma EN-50126 Ref. [1], la documentación de entrada que recibe el equipo de seguridad y la documentación de seguridad que ha de ser generada.

4.2 Ejemplo de aplicación específica

Con el fin de facilitar la comprensión de las tareas a realizar por el equipo de seguridad en cada fase, se va a utilizar un ejemplo de aplicación específica de tal manera que se puedan introducir ejemplos a la hora de explicar determinadas acciones o documentos.

El ejemplo de aplicación específica es el siguiente:

Implementación del sistema ERTMS N1 a una estación denominada "Estación Tipo". El plano de vías de dicha estación tipo se muestra en la Figura 4.2.

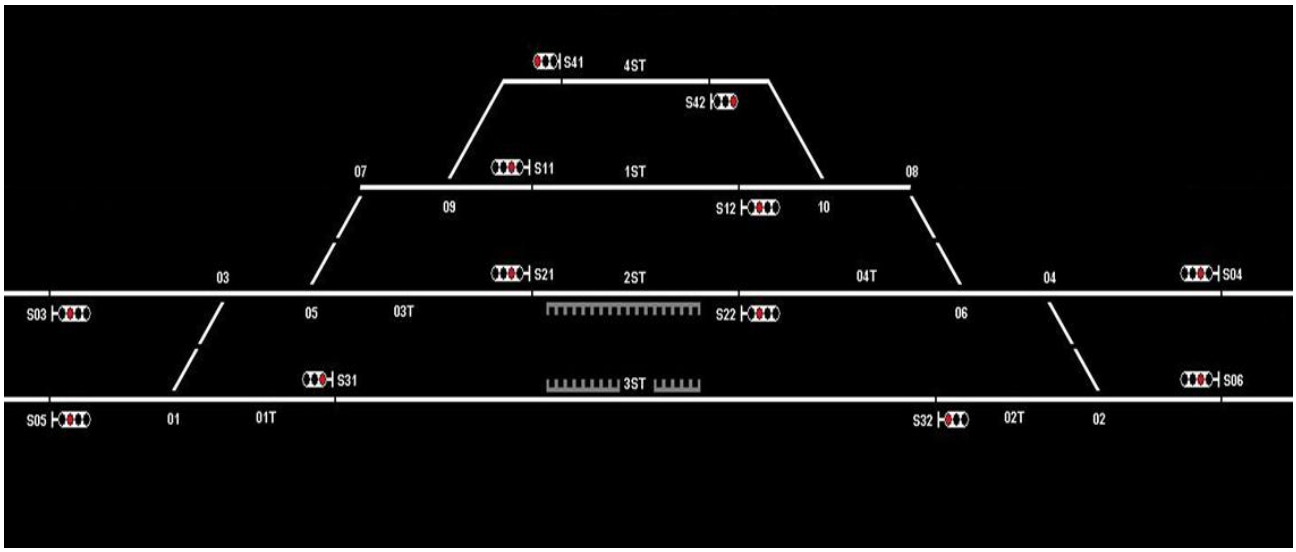


Figura 4.2. Plano de vías de Estación Tipo.

Para dicha estación se cuentan con los siguientes elementos de señalización ya descritos en el capítulo 2 del presente proyecto:

- Enclavamiento electrónico.
- Circuitos de vía.
- Señales laterales luminosas.
- Desvíos.
- CTC.

Y se quiere instalar como sistema de protección de tren el Sistema ERTMS N1. Por lo tanto se instalarán los siguientes elementos:

- Eurobalizas.
- LEUs.
- CLCs.
- Equipo embarcado ERTMS.
- Equipo de control de LTVs:

- PCE
- GR

En caso que sea necesario se hará referencia a este ejemplo de aplicación específica en los siguientes apartados de tal manera que la labor del equipo de seguridad quede lo más clara posible.

4.3 Fase I: Concepto y Definición

La fase de concepto y definición es la primera fase del ciclo de vida. En ella se ponen las bases para poder alcanzar un nivel de comprensión del sistema suficiente para permitir que todas las tareas RAMS de las siguientes fases se puedan establecer satisfactoriamente.

4.3.1 Objetivos a alcanzar en la fase

Los objetivos de esta fase de Concepto y Definición son:

- Definir el perfil de la misión del sistema.
- Definir la frontera del sistema.
- Establecer las condiciones de aplicación que influyen en las características de sistema.
- Definir el alcance del análisis de amenazas del sistema.
- Establecer la política RAMS del sistema.
- Establecer el Plan de Seguridad del sistema.

4.3.2 Documentación de entrada

La documentación de entrada para la fase de concepto y definición es:

- **Definición del Sistema**

Documento en el que se especifican a alto nivel los sistemas que componen la aplicación específica así como el alcance de la misma. Además se definen las interacciones de los componentes del sistema entre sí a través de sus interfaces, tanto internas como externas.

Utilizando el ejemplo tipo, el documento de definición del sistema contendría al menos la siguiente información:

1. Ámbito:

   Se identifica el lugar exacto en el que se va a instalar la “Estación tipo” y la línea ferroviaria a la que va a pertenecer. Así como sus fronteras, es decir, los sistemas colindantes.

2. Descripción de los elementos del sistema suministrados, en este caso equipamiento ERTMS N1:

- Componente CLC: Este componente permite recibir los estados de los elementos de campo desde el enclavamiento para su posterior procesamiento y generación de informaciones para el sistema ERTMS N1.

- Componente LEU: Este componente genera los telegramas para el sistema ERTMS N1 en función del estado de los elementos. El telegrama que se envía debe de cumplir las especificaciones UNISIG tanto en el protocolo de comunicaciones como en los datos que se envían.

- Componente Eurobaliza: Este componente envía los telegramas generados por el LEU. Al pasar por encima de una eurobaliza, la antena la magnetiza al estar dentro de su radio de acción y el telegrama es transmitido a través de la antena al equipo embarcado.

- Equipo embarcado ERTMS/ETCS: El sistema ETCS embarcado recibe la información al tren sobre autorizaciones de movimiento, velocidades máximas permitidas, características de la vía, etc. que proceden de las balizas (eurobalizas) que forman parte del sistema de señalización (para ETCS N1).

- Equipo de Control ERTMS: Este equipo permite el establecimiento y la anulación de Limitaciones Temporales de Velocidad.

3. Descripción de los interfaces:

   - Enclavamiento-CLC.

   - CLC-CLC adyacente.

   - LEU-Eurobaliza.

   - Eurobaliza-Equipo embarcado ETCS.

   - Sistema de señalización-Infraestructura.

4. Misión del sistema de señalización:

   - Misión del sistema de protección de Tren ERTMS: Ordenar por medio de la señalización la velocidad permitida en cada punto, teniendo en cuenta las informaciones recibidas desde el enclavamiento.

- **Plan de calidad**

En este documento se describen las actividades a realizar por parte del equipo de calidad para asegurar que se han seguido durante todo el ciclo de vida del proyecto la normativa de calidad especificada por la empresa encargada de la obra.

El contenido de este documento es distinto para cada empresa suministradora ya que debe contener la estrategia de calidad definida internamente por dicha empresa.

4.3.3 Documentación de seguridad a generar

La documentación a generar por parte del equipo de seguridad es:

- **Plan de seguridad**

El propósito del plan de seguridad es definir las actividades de seguridad necesarias y el plan gestión para asegurar que los subsistemas desarrollados y suministrados para la instalación se aplican correctamente.

Para el ejemplo tipo, el plan de seguridad contendría:

1. Definición del sistema:

   En este apartado se describe el sistema suministrado y de manera parecida al documento de definición del sistema, se define el perfil de la Misión de los subsistemas que componen el sistema.

   En este caso se volverían a definir las Eurobalizas, los CLCs, los LEUs y el equipo de control de LTVs.

   Además se aporta el listado de los componentes junto con su nivel de integridad de seguridad. Por ejemplo el mostrado en la Tabla 4.1.

Componente	Definición	Propuesta de SIL
Eurobaliza	Componente pasivo que envía información al equipo embarcado ERTMS cuando pasa sobre ella	SIL 0
LEU	Codificador (*Lineside Encoder Unit*)	SIL 4
CLC	Controlador de LEUs Centralizado	SIL 4

Tabla 4.1. Ejemplo de propuesta de nivel de integridad por componentes.

   Por último se definen las interfaces de seguridad entre los diferentes componentes suministrados. A la hora de definir estas interfaces, se deben declarar los canales de comunicación utilizados así como los protocolos propios definidos por cada empresa suministradora. En nuestro ejemplo, las interfaces a definir serían:

   - Westrace-CLC
   - CLC-LEU
   - CLC-CLC (adyacente)

- LEU-Baliza
- PCE-GR
- LEU-GR
- PCE-CLC

2. Gestión de la seguridad:

   En este punto, se describen la política de seguridad establecida por la empresa suministradora, así como la sistemática de la gestión de la seguridad. Lo habitual es que se trate de un proceso de gestión de riesgos con el fin de conseguir los objetivos de seguridad.

   Para ello se define claramente cuál es el proceso de gestión de la seguridad que ha de seguirse durante la consecución de la obra: la evaluación de riesgos, los criterios de aceptación de riesgos, las acciones correctoras ante no-conformidades, las auditorias que sean necesarias a lo largo del ciclo de vida, etc.

   Además se incluye en este apartado una organización del personal humano que va a trabajar en la obra. En esta organización, se establecen los roles y las responsabilidades de cada uno: Desde los Jefes de Seguridad hasta los Ingenieros de Seguridad.

3. Planificación y programación:

   Se establece una programación de las actividades de Seguridad a lo largo del ciclo de vida del sistema. Por lo que se establecen dichas actividades organizándolas en cada fase del ciclo.

- **Plan de Validación y Verificación**

El objetivo del plan de Validación y Verificación es el de definir las actividades de verificación y validación necesarias para asegurar que los componentes que integran el sistema cumplan con los requerimientos de seguridad.

Este documento deberá contener:

1. Plan de Verificación:

   El plan de verificación pretende demostrar que para las entradas de información específicas, las entregas generadas para cada fase del ciclo de vida cumplen con los requisitos de la fase que se está analizando.

   Para ello en este documento se establece un listado de actividades de verificación tanto a nivel global como específicas para cada fase que dependerá de cada empresa suministradora.

   Al final del ciclo de vida será necesario generar un informe de Verificación en el que aparezcan las actividades definidas en el plan de tal manera que se pueda comprobar si se han ido cumpliendo o no.

2. Plan de Validación:

   La validación es la actividad por la que se confirma, mediante examen y aportación de pruebas objetivas, que se cumplen los requisitos pretendidos.

   En este plan se establecen las pruebas que van a ser necesarias tanto en laboratorio como en campo para poder comprobar que los datos programados son los correctos.

   En el caso de ejemplo, se definirán una serie de protocolos de pruebas relacionadas con el Sistema ERTMS Nivel 1 que deberán ser pasadas con éxito.

4.4 Fase II: Análisis de riesgos.

La fase de análisis de riesgos es una de las de mayor importancia de todo el ciclo de vida ya que la correcta implementación del proceso de gestión de amenazas y control de riesgos de la aplicación es fundamental para evitar situaciones de peligro.

Este proyecto solo se centra en los riesgos y amenazas de la aplicación específica ya que las amenazas genéricas de cada producto utilizado (LEU, PCE, PLO-R, GR, etc.) ya están cubiertas dentro de cada Caso de Seguridad Genérico equivalente. Esto quiere decir que se da por supuesto que un producto genérico no va a producir situaciones de peligro por sí solo. Lo que es necesario estudiar son las posibles amenazas que puedan surgir al implementar todos estos productos dentro de una aplicación específica concreta.

Esta fase no se va a cerrar hasta que se termine el proyecto, ya que pueden surgir nuevas amenazas a medida que el proyecto avance, y por tanto, sea necesario gestionarlas y mitigar sus riesgos asociados.

4.4.1 Objetivos a alcanzar en la fase.

Los objetivos a alcanzar en esta fase son:

- Identificar las amenazas asociadas al sistema.
- Identificar las circunstancias que nos conducen a amenazas.
- Determinar el riesgo asociado a cada una de las amenazas.
- Establecer un proceso para la gestión del riesgo continua.

4.4.2 Documentación de entrada.

La documentación que sirve de entrada en esta fase es la que se ha generado en la fase anterior. Principalmente se utiliza como punto de partida el Plan de Seguridad y el documento de Definición del Sistema.

4.4.3 Documentación a generar.

La documentación a generar por parte del equipo de seguridad en esta fase es:

- **Análisis preliminar de Riesgos (APR)**

El objetivo del análisis preliminar de riesgos es identificar, clasificar y asignar riesgos a todas las posibles situaciones que, individualmente o en combinación con otras, podrían potencialmente causar un accidente.

Dentro de este análisis se justifica el SIL asignado a las funciones de seguridad de cada componente y se determinan los requisitos generales de seguridad que deben cubrir la aplicación específica determinada.

Se consideran de manera general tres accidentes potenciales: Colisión, Descarrilo y Atropello.

Lo primero que contiene este documento son los criterios de aceptación de riesgos. En el ejemplo propuesto se van a utilizar los mismos que aparecen en la norma EN-50126 Ref. [1]. Por lo tanto se tendrá:

- Niveles de Severidad: Ver Tabla 3.2 del presente proyecto.
- Niveles de Frecuencia: Ver Tabla 3.1 del presente proyecto.
- Evaluación del riesgo: Ver Tabla 3.5 del presente proyecto.

Una vez determinados los criterios de aceptación del riesgo, se establece una metodología para el análisis de riesgos. Una posible metodología sería la siguiente:

1. Se clasifican los posibles accidentes que pueden ocurrir en una explotación ferroviaria:
    a. Colisión.
    b. Descarrilo.
    c. Atropello
2. Se identifican las posibles Situaciones de Peligro que pueden tener como consecuencia cada uno de estos accidentes. Un ejemplo de situación de peligro sería:
    a. SP1: El tren circula a una velocidad excesiva.
3. Se analiza cada situación de peligro para determinar los posibles escenarios que puedan concluir a cada una de ellas. Partiendo de la anterior situación de peligro, se podrían llegar a los siguientes escenarios:
    a. SP1-1: Un tren circula a una velocidad excesiva al paso por un desvío.
    b. SP1-2: Un tren circula a una velocidad excesiva al paso por una zona de vía con limitaciones de velocidad.

    A cada uno de estos escenarios se le asigna una severidad y se establece una frecuencia de ocurrencia objetivo una vez que se hayan aplicado todas las posibles medidas mitigadoras para que el riesgo resultante se reduzca a un nivel aceptable.

En este caso la gravedad para todos los escenarios es “Catastrófica”, por lo que la frecuencia de destino debe ser, en todos los casos, “Increíble” para conseguir un nivel de riesgo “Insignificante”.

4. Para cada uno de estos escenarios se establece una Función de Seguridad de alto nivel para garantizar que se evite la ocurrencia del escenario y por tanto la Situación de Peligro y el posible accidente. En nuestro caso se podrían establecer, entre otras, las siguientes Funciones de Seguridad que deben ser satisfechas por el sistema:

    a. FS1: El sistema de señalización informará mediante un código de las condiciones bajo las que debe circular al pasar por un desvío

    b. FS2: El sistema de señalización incluirá sistemas de protección automáticos para garantizar que sean respetadas la limitaciones de velocidad temporales y permanentes.

5. Partiendo de las Funciones de Seguridad, se establecen las funciones principales que debe realizar cada uno de los Subsistemas de Seguridad suministrados.

6. Para cada una de estas funciones de seguridad de subsistemas se relacionan las funciones secundarias (a nivel de componentes) que permiten garantizar que se realiza la función de seguridad de sistema correspondiente.

    En esta segunda parte del análisis realizado a nivel de subsistemas se determinan las funciones de seguridad que realiza cada uno de los componentes para impedir la ocurrencia de las Situaciones de Peligro y posibles accidentes.

    A estas funciones de componentes se les asigna un SIL que dependerá de la severidad que supone su fallo.

7. Se detectan las amenazas que implica el no cumplimiento de estas funciones de seguridad para cada componente que se detecten.

8. Por último se determinan los Requisitos Generales de Seguridad para garantizar que se evita la ocurrencia de amenazas.

Una vez que se ha establecido la metodología de análisis de riesgos se procede a la construcción del análisis de amenazas como tal. De manera habitual se hace en formato Excel para una mejor comprensión. Siguiendo los pasos marcados anteriormente, podríamos obtener por ejemplo las siguientes tablas:

- La Tabla 4.2 muestra las posibles situaciones de peligro:

CONSECUENCIA	ID	SITUACIÓN DE PELIGRO		ESCENARIO	SEVERIDAD	FRECUENCIA OBJETIVO	RIESGO OBJETIVO	FUNCIONES DE SEGURIDAD DE ALTO NIVEL		SIL
Descarrilo	SP1	El tren circula a una velocidad excesiva	SP1-1	Un tren circula a velocidad excesiva al paso por un desvío	Catastrófica	Increíble	Despreciable	FS1	El sistema de señalización informará mediante un código de las condiciones bajo las que debe circular al pasar por un desvío	SIL 4
			SP1-2	Un tren circula a velocidad excesiva al paso por una zona de vía con limitaciones permanentes o temporales	Catastrófica	Increíble	Despreciable	FS2	El sistema de señalización incluirá sistemas de protección automáticos para garantizar que sean respetadas la limitaciones de velocidad temporales y permanentes	SIL 4

Tabla 4.2. Ejemplo de situaciones de peligro

- La
- Tabla 4.3 muestra la asignación SIL a las funciones de los subsistemas**:**

FUNCIONES DE SEGURIDAD DE ALTO NIVEL		ASIGNACIÓN SIL	SUBSITEMA	FUNCIONES PRINCIPALES (SUBSISTEMA)		DESCRIPCIÓN DE FUNCIONES		SIL	COMPONENTE / ALCANCE
FS1	El sistema de señalización informará mediante un código de las condiciones bajo las que debe circular al pasar por un desvío	SIL 4	ERTMS	FSR1	El subsistema ERTMS seleccionará el telegrama a enviar teniendo en cuenta el estado de los aparatos de vía enviados por el Enclavamiento.	FR1	Recibir informaciones sobre la ruta construida por el Enclavamiento	SIL 4	Interfaces ENCE/ERTMS CLC RBC
						FR2	Enviar a las balizas adecuadas el telegrama correspondiente según las rutas construidas por el ENCE.	SIL 4	Componentes ERTMS N1 PCE
						FR3	La Baliza enviará únicamente el mensaje recibido del LEU en cada momento. En caso de no recibir ningún mensaje enviará el telegrama por defecto.	SIL 4	Balizas LEU

			ERTMS	FSR2	El subsistema ERTMS generará la información con el objetivo de que el tren no exceda la velocidad permitida en cada punto de la ruta.	FR4	Garantizar la correcta Ubicación de las balizas ERTMS.	SIL 4	Balizas
						FR5	Enviar información más restrictiva a las balizas cuando no se recibe información del Enclavamiento	SIL 4	CLC/LEU
						FR6	Enviar información acerca del estado de la señalización a componentes ERTMS.	SIL 4	LEU,CLC I-LEU-CLC
						FR7	Generar Autorizaciones de Movimiento según las rutas establecidas por el Enclavamiento (Paquete 12)	SIL 4	Data Prep ERTMS
						FR8	Generar los datos relacionados con las limitaciones temporales de velocidad.	SIL 4	Data Prep ERTMS GR

Tabla 4.3. Ejemplo de Asignación SIL a funciones de subsistema.

- La Tabla 4.4 muestra la detección de amenazas del subsistema ERTMS: (utilizando como ejemplo las funciones de subsistema FR1 y FR2)

FUNCIONES		ID AMENAZA	AMENAZAS	COMPONENTE
R1	Recibir informaciones sobre la ruta construida por el Enclavamiento	AM_ERTMS001	El sistema ERTMS N1 envía al tren un telegrama incorrecto debido a defectos en el interfaz de datos entre el ENCE y ERTMS N1.	Interfaz ENCE/ERTMS N1
		AM_ERTMS002	Pérdida de la ruta establecida por el enclavamiento por fallo en las comunicaciones ENCE/CLC	Interfaz ENCE/ERTMS N1
		AM_ERTMS003	Pérdida de la ruta establecida por el enclavamiento por fallo o reinicio del CLC	CLC
		AM_ERTMS004	Pérdida de la ruta establecida por el enclavamiento por fallo en las comunicaciones ENCE/RBC	Interfaz ENCE/RBC
		AM_ERTMS005	Pérdida de la ruta establecida por el enclavamiento por caída o reinicio del RBC	RBC
R2	Enviar a las balizas adecuadas el telegrama correspondiente según las rutas construidas por el ENCE.	AM_ERTMS006	Fallo en las comunicaciones entre el LEU y las balizas.	interfaz LEU-Balizas C
		AM_ERTMS07	Pérdida de la comunicación entre el CLC y el LEU	interfaz CLC-LEU
		AM_ERTMS08	Versiones entre LEU/CLC son incorrectas	LEU

				CLC
		AM_ERTMS09	Mantenimiento del CLC en desacuerdo con su manual de mantenimiento	CLC
		AM_ERTMS010	Mantenimiento del LEU en desacuerdo con su manual de mantenimiento.	LEU
		AM_ERTMS011	Mantenimiento del PCE en desacuerdo con su manual de mantenimiento.	PCE
		AM_ERTMS012	La instalación de armarios CLC/LEU es errónea	LEU
				CLC
		AM_ERTMS013	Error de conexionado de las balizas	Balizas C
		AM_ERTMS014	Las balizas no se instalan de acuerdo a la Tira de Vía	Balizas C
		AM_ERTMS015	Distribución de balizas de relocalización sin tener en cuenta las necesidades de los odómetros	Balizas
		AM_ERTMS016	El sistema ERTMS N1 envía al tren un telegrama incorrecto debido un fallo genérico del LEU	LEU
		AM_ERTMS017	El sistema ERTMS N1 envía al tren un telegrama incorrecto debido un fallo genérico del CLC	CLC

Tabla 4.4. Ejemplo de establecimiento de amenazas a funciones de subsistema.

- **Registro de Amenazas (*Hazard Log*)**

El objetivo del *Hazard Log* es el de recoger, dentro de un mismo documento, todas las amenazas que se hayan identificado en el Análisis Preliminar de Riesgos. Además, se incluirán las posibles amenazas que surjan a lo largo del desarrollo del proyecto y que no hayan sido identificadas en el APR. Es por eso que el *Hazard Log* es un documento vivo a lo largo de toda la obra ya que se va a ir actualizando a medida que se avance en las fases del ciclo de vida.

La estructura básica del *Hazard Log* es la siguiente:

- Amenazas:

    1. Se listan todas las amenazas encontradas en el APR.

    2. Se relaciona cada amenaza con un requisito de seguridad. Los requisitos de seguridad se generan en la siguiente fase (III).

    3. Se establece un nivel de riesgo inicial.

    4. Se determinan las medidas de mitigación necesarias para cada amenaza.

    5. Se establece un nivel de riesgo residual tras el uso de las medidas de mitigación.

    6. Si no se puede relacionar la amenaza con un requisito, o no existe ninguna medida de mitigación que haga que el riesgo residual sea Despreciable, será necesario exportar dicha amenaza como Riesgo Exportado a la Autoridad Ferroviaria.

- Riesgos Exportados:

    En el apartado de riesgos exportados se detallan todos los posibles riesgos que no haya sido posible mitigar y que por tanto no se pueden considerar despreciables. Se ha de definir la situación de riesgo que se exporta a la autoridad ferroviaria y el nivel de riesgo existente, ya se Intolerable o Tolerable.

- Condiciones de Uso:

    En el apartado de condiciones de uso se enumeran una serie de condiciones que se deben tener en cuenta a la hora de llevar a cabo la explotación de la línea.

    Una situación típica en la que sea necesaria establecer una condición de uso seria la siguiente: La empresa suministradora del sistema diseña un procedimiento para establecer o quitar Limitaciones Temporales de Velocidad. Sin embargo es el operador el encargado de establecer o quitar dichas limitaciones en la práctica; por tanto una condición de uso que se podría establecer sería:

CU-1: El Operador ha de tener en cuenta el Procedimiento de Gestión de LTVs en el establecimiento y anulación de las mismas.

- Restricciones Temporales de Servicio:

  En el caso de que sea necesario generar alguna restricción sobre el sistema de manera temporal, habrá que establecer una Restricción Temporal de Servicio. Se trata de una condición que se le impone al operador pero que no va a permanecer durante toda la vida del sistema, sino que se va a modificar para poder eliminar dicha restricción.

  En el caso del ejemplo de aplicación establecido, podría ocurrir que en la Vía 4 no se han instalado aún las eurobalizas de ERTMS. Por tanto si un tren circulase por esa vía con el sistema ERTMS a bordo encendido, podría suponer una situación de riesgo. En ese caso se establecería una Restricción Temporal de servicio en la que se especificase que en la Vía 4 no se puede circular bajo el sistema ERTMS debido a que no existen balizas para asegurar las circulaciones. Esta restricción se eliminaría del *Hazard Log* una vez que se hayan instalado las balizas que faltan en la vía 4.

4.5 Fase III: Especificación de Requisitos.

En la fase de especificación de requisitos, aparte de generar los requisitos de seguridad provenientes del estudio realizado en el Análisis Preliminar de Riesgos, se van a definir las funcionalidades necesarias para el sistema.

4.5.1 Objetivos a alcanzar en esta fase.

Los objetivos de esta fase son:

- Especificar la totalidad de requisitos RAMS del sistema.
- Especificar la totalidad de criterios de demostración y aceptación para las RAMS del sistema.
- Establecer el Programa RAM para controlar las tareas RAM en las subsiguientes fases del ciclo de vida.
- Trazabilidad de la totalidad de los requisitos RAMS, desde el sistema a los subsistemas, componentes e instalaciones externas.
- Definir el criterio de aceptabilidad RAMS para los subsistemas, componentes e instalaciones externas.

4.5.2 Documentación de entrada.

La documentación de entrada con la que trabaja el equipo de seguridad es la siguiente:

- **Especificación de requisitos.**

En el documento de especificación se recogen todos los requisitos de seguridad de obligado cumplimiento por el sistema. Estos requisitos se obtienen en la anterior fase, en el Análisis Preliminar de Riesgos.

Aparte de los requisitos de seguridad provenientes de la fase de análisis de riesgos, se pueden incluir en este documento otros requisitos que no afecten a la seguridad pero si al funcionamiento del sistema. En este caso se habla de requisitos funcionales, los cuales pueden ser establecidos por la propia empresa suministradora o por el cliente en el caso de tener una necesidad específica.

La especificación de requisitos se dividirá en cada subsistema (CLC, LEU, Baliza, PCE, etc.) y también se dividirá en funcionalidades del sistema (Transiciones, Perfil estático de velocidad, perfil de gradiente, autoridad de movimiento, etc.)

A partir del APR de ejemplo que se ha generado en el anterior apartado, se podrían obtener, entre otros muchos, los siguientes requisitos:

- Requisito del LEU: Cada LEU recibirá de un único CLC, la parte de información de señalización que necesita para seleccionar los telegramas. En caso de pérdida de comunicación entre el CLC y el LEU, todas las variables intercambiadas entre estos dos equipos pasan a estar desactivadas. En la aplicación ERTMS el LEU recibirá del CLC información sobre:

    - Aspecto de las señales *(Proceed, On Sight, Shunting*).

    - Posición de los desvíos (Derecha, Izquierda).

- Requisito de Autoridad de Movimiento (MA): La longitud de la Autoridad de movimiento dependerá de los aspectos de las señales que conforman la ruta establecida y del funcionamiento de los CLC´s asociados a dichas señales, así como del funcionamiento de IR´s colaterales. En condiciones normales de funcionamiento, es decir, sin fallos en los equipos, esta autoridad de movimiento será calculada por la herramienta de preparación de datos. En caso de existir fallo en CLC o IR, será este último el que genere la correspondiente repercusión por fallo (acortamiento de MA).

- **Especificación de Interfaces**

En el documento de especificación de interfaces se detallan las interacciones entre los subsistemas. Se determinan tanto el tipo de información que intercambian como los canales de comunicación que deben utilizar para que el funcionamiento sea el correcto.

Dependiendo de los subsistemas que compongan el sistema, este documento incluirá más o menos interfaces.

- **Especificación de Fronteras ETCS**

El objetivo del documento de especificación de fronteras ETCS es el de definir las áreas equipadas con ETCS dentro del sistema. Además se establecen las transiciones de entrada y de salida al sistema ERTMS. Al establecer estas transiciones no sólo se determinan las señales de entrada y de salida del sistema, sino que también se definen las velocidades de transición y si existe anuncio previo o si se transita inmediatamente al pasar por la baliza que envía el paquete de transición de nivel.

4.5.3 Documentación a generar.

La documentación que debe generar el equipo de seguridad es:

- **Informe de seguridad de Interfaces**

El equipo de seguridad debe revisar las especificaciones de cada interfaz y generar este informe de seguridad en el que se estudien las amenazas que se pueden generar en dicho interfaz y los modos de fallo de los componentes que lo forman.

De esta manera, se debe asegurar que en caso de fallo en el interfaz, no se genera una situación de peligro, sino que el sistema pasa a un estado más seguro.

Así por ejemplo, en el caso del interfaz ENCE-CLC, si se pierde la comunicación, el CLC deja de mandar la información de las señales y los desvíos, por lo que las balizas mandan el telegrama por defecto que hace que el tren se detenga.

- **Auditoría de documentación de entrada para el diseño. (Baseline)**

La auditoría de documentación de entrada para el diseño es una actividad que debe realizar el equipo de seguridad para corroborar que la documentación que ha generado la empresa suministradora para el diseño del sistema son los adecuados y se corresponden con los recogidos en la definición del sistema.

Para realizar la auditoría se debe seguir una metodología, un ejemplo de esta metodología sería la siguiente:

- Se comprueba por cada uno de los documentos definidos en la Definición del Sistema, los siguientes puntos:

  - Título: Comprobación de que coinciden el título del documento y el referenciado en el documento de Definición del Sistema.

  - Código: Comprobación de que la codificación del documento existe y coincide con la del documento de Definición del Sistema.

  - Edición: Comprobación de que la versión referenciada en la documentación de diseño coincide con la referenciada en el documento de Definición del Sistema.

  - Fecha: Comprobación de que la fecha referenciada en la documentación de diseño coincide con la referenciada en el documento de Definición del Sistema.

  - Existencia del documento: Comprobación de que el documento existe físicamente y que se encuentra disponible para los responsables del diseño del sistema suministrado.

  Si existen evidencias de que se han utilizado estos documentos como base de partida para el diseño, el resultado se marca como satisfactorio (OK). Si no existen evidencias se abre una No-Conformidad (NC).

Con esta metodología se genera una *checklist* en la que se introducen todos los puntos de control y se van incluyendo uno por uno cada documento recogido en la Definición del Sistema.

4.6 Fase IV: Diseño y Desarrollo.

En la fase de diseño y desarrollo, la empresa suministradora del sistema de señalización debe generar toda la programación de datos que se cargan en los diferentes equipos que forman el propio sistema.

4.6.1 Objetivos a alcanzar en esta fase.

Los objetivos de esta fase son:

- Crear subsistemas y componentes conforme a los requisitos.
- Demostrar que los subsistemas y componentes son conformes a los requisitos RAMS.
- Establecer planes para las tareas futuras del ciclo de vida concernientes a RAMS.

4.6.2 Documentación de entrada.

El equipo de seguridad debe revisar la siguiente documentación de entrada generada por los distintos equipos de ingeniería de la empresa suministradora:

- **Tira de vía**

Es el plano en el que se representa la vía. Debe incluir todos los elementos de vía que componen el sistema (Señales, Circuitos de Vía, Eurobalizas, Desvíos)

En la Figura 4.3 se muestra el detalle de una tira de vía:

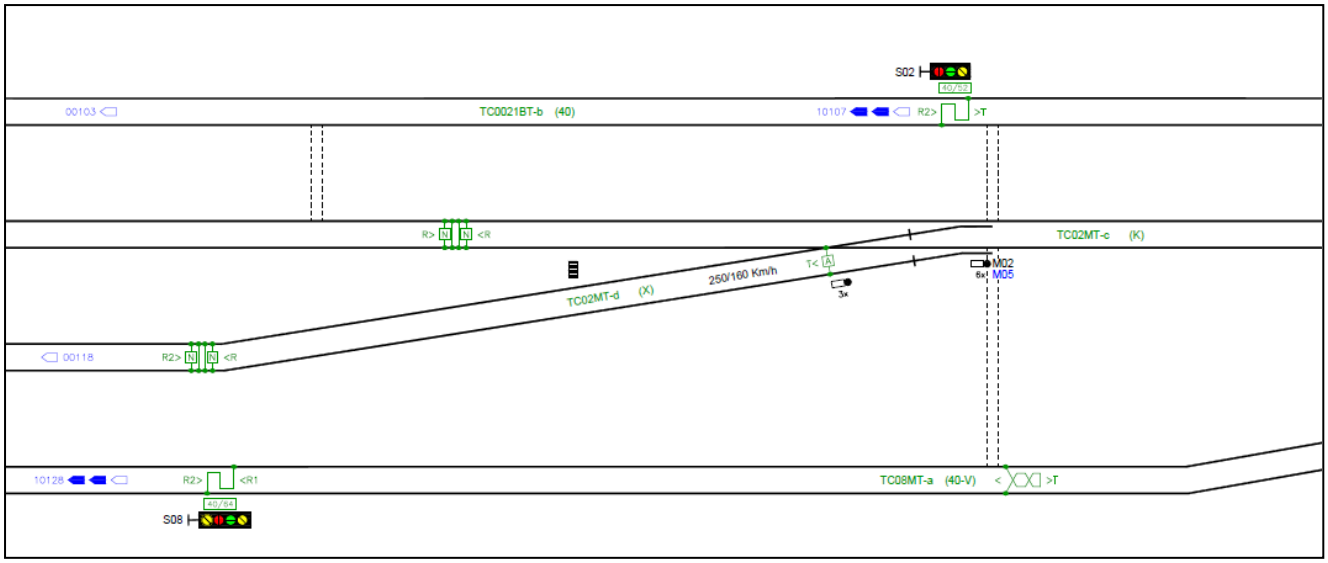


Figura 4.3. Detalle de una tira de vía

- **Informe de auscultación**

Para la programación del sistema ERTMS, es necesaria la realización de auscultaciones de vía para conocer el punto kilométrico de cada uno de los elementos necesarios para la programación ERTMS: señales, balizas ERTMS, agujas, piquetes de agujas, circuitos de vía, etc.

El sistema ERTMS necesita saber las distancias reales a los eventos que le afectan. Por lo tanto se pretende disponer de una tabla donde estén reflejados los puntos kilométricos de cada elemento en campo.

En muchas ocasiones, la información que proporciona el cliente a la empresa suministradora no es exacta, y eso provoca que la empresa suministradora deba hacer una auscultación propia y determinar un margen de seguridad para aceptar que el punto kilométrico es el correcto. En caso de que la diferencia entre lo auscultado y lo remitido por el cliente sea superior a ese margen de seguridad, será necesario llevar a cabo una segunda auscultación del elemento. Un margen habitual es el de ± 1,5 metros.

En la Tabla 4.5 se muestra un ejemplo de auscultación de elementos y su comparación con lo marcado en la tira de vía proporcionada por el cliente:

EVENTO REAL	NOMBRE	PK AUSCULTADO	PK AUSCULTADO CORREGIDO	PK DE TIRA	ERROR (m)
NON_CONTROLLED_ BALISE	S12	4797,25	4802	4802	**0**
SEÑAL	S12	4803	4807,71	4807	**-0,71**
CIRCUITO DE VÍA	1ST	4813	4817,64	4817	**-0,64**
AGUJA	03T	5258,75	5260,06	5259	**-1,06**
CIRCUITO DE VÍA	2ST	5334,63	5334,63	5334	**-0,63**
CIRCUITO DE VÍA	04T	5566	5564,99	5566	**1,01**
SEÑAL	S22	5576	5574,92	5576	**1,08**

Tabla 4.5. Ejemplo de Auscultación de Elementos.

- **Informe de gradiente**

Al igual que con la ubicación exacta de los elementos, es necesario saber el perfil de gradiente de la vía. De tal manera que el sistema ERTMS sea capaz de calcular las curvas de frenado del tren ya que la curva de frenado es más larga si un tren recorre un gradiente de pendiente (plano inclinado descendente) que un gradiente de rampa (plano inclinado ascendente)

La empresa suministradora recibe del cliente una información de gradiente, y para corroborarla realiza una auscultación propia. Al igual que antes, si las diferencias encontradas no se consideran aceptables, se procederá a una segunda auscultación.

En la Figura 4.4 y en la Figura 4.5 se muestran varios ejemplos de auscultaciones de gradiente. En la Figura 4.4 se ve como la información auscultada y la proporcionada por el cliente son coincidentes, mientras que en la Figura 4.5 se ve que los datos no son coincidentes.

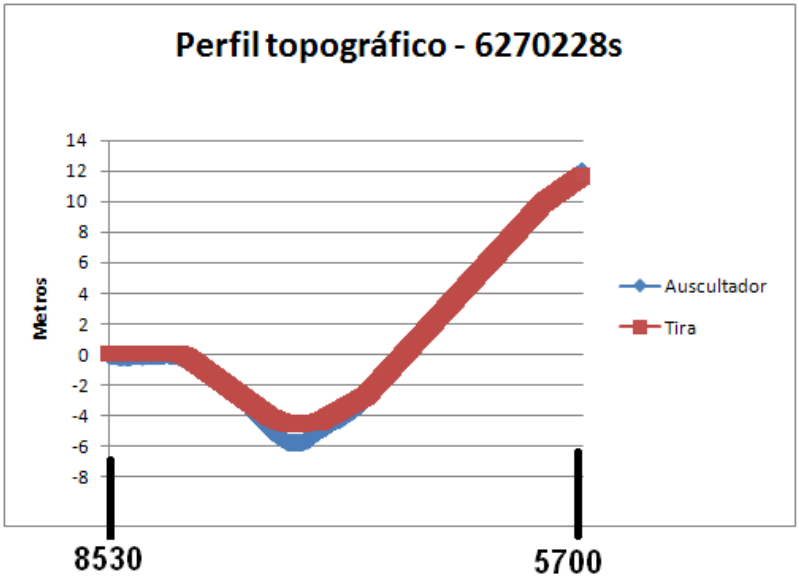


Figura 4.4. Auscultación de gradiente. Gradientes coincidentes.

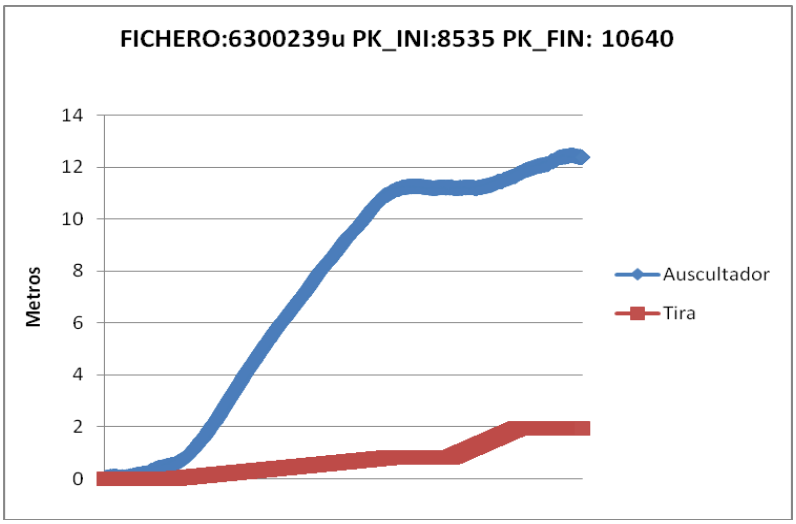


Figura 4.5. Auscultación de gradientes. Gradientes no coincidentes.

- **Protocolo de pruebas en laboratorio de datos (LEUs y Balizas)**

El propósito del protocolo de pruebas es recoger el conjunto de pruebas a las que hay que someter al sistema ERTMS para la validación de la funcionalidad del sistema ERTMS a implantar.

Los distintos apartados que componen este protocolo de pruebas comienzan con una descripción de las pruebas a realizar y finalizan con una Hoja de Registro en la cual se cumplimentará el resultado de las distintas pruebas efectuadas.

Existe trazabilidad entre las pruebas definidas en este protocolo de pruebas y la especificación de requisitos de aplicación del sistema ERTMS N1.

Además de la especificación de las pruebas que son necesarias realizar para validar los datos del sistema, se determina el entorno de pruebas de laboratorio que se va a utilizar, como por ejemplo el que se muestra en la Figura 4.6:

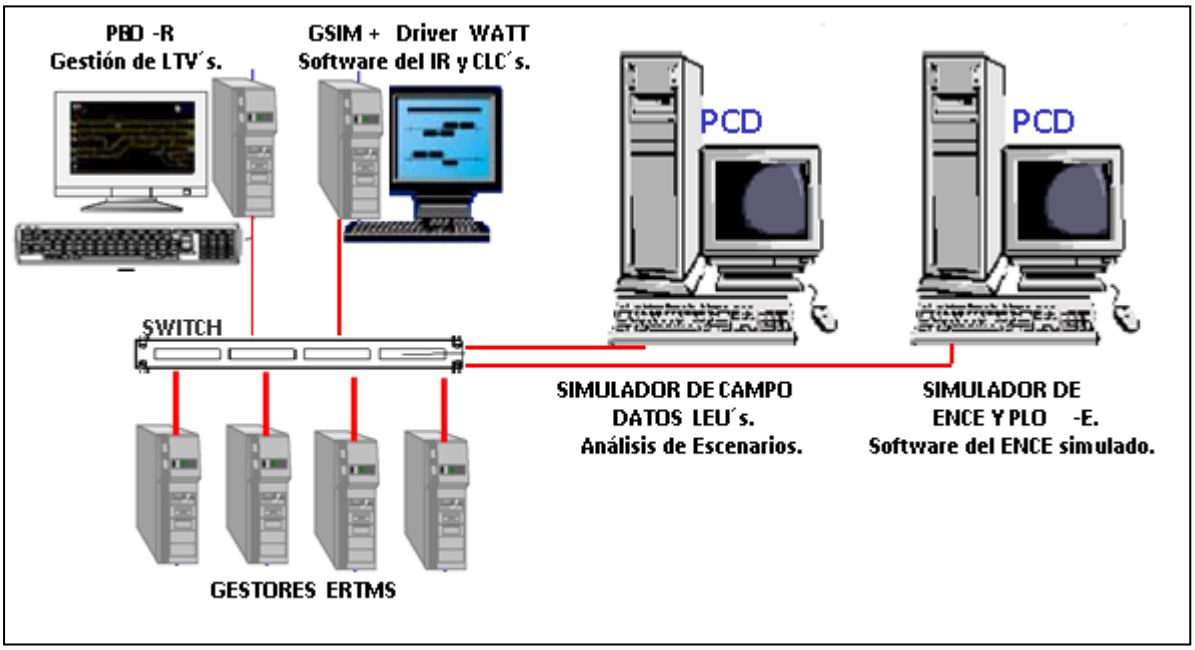


Figura 4.6. Ejemplo de entorno de pruebas de simulación.

Este entorno de pruebas software, permitirá realizar todas aquellas pruebas que no dependan de otros sistemas, es decir, está confeccionado para verificar la programación de datos del sistema ERTMS N1. Evidentemente, para la realización de las pruebas correspondientes a la integración con los sistemas ENCE, PCE, SAM,... será necesaria la utilización de otro entorno más completo en donde los sistemas antes mencionados estén comunicados con el sistema ERTMS N1 a través de una red de comunicaciones. Una vez que estos sistemas están integrados y comunicados, la única prueba a realizar consistirá en verificar los datos del interfaz.

En estas pruebas es necesario probar las siguientes funcionalidades:

- Perfiles Estáticos de Velocidad. SSP.
- Perfiles de Gradiente.
- Enlace entre grupos de balizas. *Linking*.
- Autoridad de Movimiento.
- Rebase Autorizado. Modo *On sight*.
- Maniobras. *Modo Shunting*.
- *Stop If In Staff Responsible* Mode.
- *Timers* de Sección.
- Información Geográfica.
- Transiciones de Nivel.

- Valores Nacionales.
- Mensajes de Texto.
- Telegrama por defecto.
- Limitaciones Temporales de Velocidad
- Fallos en el Sistema. Repercusiones.
- Gestión del Mando.
- Sonería por fallos o averías.

A continuación se muestra la definición de alguna prueba que es necesario realizar relacionado con la Autoridad de Movimiento y las rutas simples:

1. Con ruta simple establecida, se comprobará que los MA generados para el grupo de balizas *main* e *infill* de la señal origen de la ruta, son coincidentes en el EoA.

2. Se comprobará que los MA generados para el grupo de balizas *main* e *infill* de la señal destino de la ruta (señal en rojo), son coincidentes en el EoA.

3. Si la información del EoA presente en las distintas balizas (de las señales origen y destino) son coincidentes, se anotará el valor del PK absoluto del EoA que deberá coincidir con el esperado. El EoA se ubicará en la misma señal.

4. Se comprobará que los *Danger Point* (DP) generados para el grupo de balizas *main* e *infill* de la señal origen de la ruta, son coincidentes.

5. Se comprobará que los *Danger Point* (DP) generados para el grupo de balizas *main* e *infill* de la señal destino de la ruta, son coincidentes.

Una vez realizadas las pruebas definidas en el protocolo, se procede a rellenar la Hoja de Registro en el que quedan los resultados obtenidos de cada prueba. En el caso de las pruebas especificadas anteriormente, se podría obtener el registro mostrado en la Tabla 4.6:

	AUTORIDAD DE MOVIMIENTO					
	Id Ruta / Nº prueba	1	2	3	4	5
01	I S03 → S12	√	√	17324	√	√
02	I S03 → S22	√	√	21301	√	√
03	I S03 → S42	√	√	18718	√	√

Tabla 4.6. Ejemplo de Hoja de Registro.

- **Pruebas en laboratorio de interfaces**

Existen pruebas que afectan a varios subsistemas y que no pueden ser realizadas en el entorno de laboratorio descrito anteriormente. Por esa razón, es necesario realizar pruebas específicas para cada Interfaz definido en el sistema.

Estas pruebas dependerán de los subsistemas que componen el sistema general y en general serán pruebas de comunicación entre los subsistemas y de envío y recepción de datos de manera segura.

- **Protocolo de pruebas en laboratorio sistema de control de LTVs**

El objetivo del protocolo de pruebas en laboratorio del sistema de control de LTVs es definir las pruebas a realizar en fábrica de los datos del PCE con la instalación.

En concreto, se pretende verificar:

- El adecuado reflejo de indicaciones generadas por la instalación en el PCE.
- La correcta ejecución de las órdenes sobre la instalación.
- La representación de las LTV activas en la pantalla de textos.

Las pruebas se pueden dividir en cuatro grandes grupos:

- Prueba de comprobación de versiones de datos.

  Con la prueba de comprobación de versiones de datos se pretende verificar que la versión de datos del GR y PCE es la misma.

  La prueba se considera válida si en el arranque de los distintos sistemas, el PCE no informa de que los datos son erróneos cuando recibe la inicialización del GR y la versión de datos coincide, y que informa del error en caso contrario.

- Prueba de integración con el módulo IR.

La prueba de integración con el módulo IR consiste en la comprobación de que todos los elementos del módulo IR se representan correctamente en el PCE, así como que los mandos realizados sobre dicho módulo se ejecutan adecuadamente.

La prueba se considera válida si el módulo IR acepta los mandos enviados desde el PCE y la ejecución de dichos mandos afecta correctamente a los elementos representados de dicho módulo.

- Prueba de integración con el módulo GR.

La prueba de integración con el módulo GR consiste en la comprobación de que todos los elementos del módulo GR se representan correctamente en el PCE, así como que los mandos realizados sobre dicho módulo se ejecutan adecuadamente.

La prueba se considera válida si el módulo GR acepta los mandos enviados desde el PCE y la ejecución de dichos mandos afecta correctamente a los elementos representados de dicho módulo.

- Prueba de funcionalidad

Con la prueba de funcionalidad se pretende comprobar la respuesta del sistema PCE ante ciertas condiciones especiales incluidas en la funcionalidad del mismo.

La prueba se considera válida si el PCE se comporta para los casos descritos según lo establecido en los requisitos del sistema.

La Tabla 4.7 muestra algún ejemplo de pruebas a realizar:

Acción	Criterio de Aceptación	Comentarios
Arrancar todos los sistemas y verificar que se conectan entre sí.	Tanto en el PCE como en el PLE representan correctamente los estados del sistema ERTMS.	OK
Verificar visualmente que las balizas se representan correctamente.	El PCE muestra las balizas en la misma posición que el PLE.	OK
Provocar la pérdida de comunicación de una baliza con el GR.	El PCE muestra la baliza en amarillo intermitente.	OK
Provocar el estado de descarga de LTV en una baliza.	El PCE muestra la baliza en amarillo fijo.	OK

Tabla 4.7. Ejemplo de pruebas del sistema de control de LTVs.

4.6.3 Documentación a generar.

El equipo de seguridad debe revisar toda la documentación de entrada generada en esta fase. Comprobará que se han realizado todas las pruebas necesarias y actualizará el *Hazard Log* en caso necesario. Además deberá realizar la auditoría de Diseño de aplicación del Sistema.

- **Auditoría de diseño**

El objetivo fundamental de esta auditoría de diseño es comprobar que las actividades de seguridad para las fases de Especificación técnica y funcional, Diseño y Desarrollo y Producción cumplen los requisitos establecidos en los Planes Particulares de Seguridad y en el Plan General de Seguridad.

En concreto en esta auditoría se comprueba si:

- Se han seguido las directrices del Plan General de Seguridad en lo que se refiere al diseño de la aplicación específica.

- Los componentes genéricos utilizados son adecuados desde el punto de vista de seguridad para la aplicación específica y disponen de la documentación que avala la seguridad del producto genérico.

- Los requisitos de seguridad identificados son el punto de partida para el diseño de la aplicación y están trazados al diseño realizado para cada componente.

La metodología a utilizar es la de utilización de un cuestionario tipo Lista de Chequeo en el que se recogen las evidencias que demuestran el cumplimiento de las directrices del Plan de Seguridad para cada uno de los componentes suministrados para el alcance del proyecto.

La Tabla 4.8 muestra un ejemplo de *checklist* utilizado para llevar a cabo la auditoría:

ID	Diseño y desarrollo	SI / NO	Evidencias	Comentarios
1	¿Cumple el diseño efectuado los requisitos de seguridad Establecidos para cada componente?			
2	¿Cumplen los interfaces los requisitos de integridad de seguridad establecidos?			
3	¿Se han modificado el diseño durante el proyecto para mitigar alguna amenaza?			
4	¿Son adecuados los métodos, herramientas y Técnicas empleados para el diseño de la aplicación específica?			

Tabla 4.8. Ejemplo de *Checklist* para Auditoría de Diseño.

4.7 Fase V: Producción.

Una vez que se ha hecho el diseño tanto de los equipos como de los datos y estos han sido probados en laboratorio. Se procede a la fabricación de los subsistemas que la empresa va a suministrar a la obra.

4.7.1 Objetivos a alcanzar en esta fase.

Los objetivos de esta fase son:

- Implementar un proceso de fabricación que dé lugar a subsistemas y componentes válidos en términos de RAMS.

- Establecer un conjunto de directrices que aseguren que los procesos están centrados en RAMS.

- Establecer unas pautas que den soporte a las RAMS de los subsistemas y componentes.

4.7.2 Documentación de entrada.

La documentación que genera la empresa suministradora y debe ser revisada por el equipo de seguridad es:

- **Hoja de registro de datos de Fabricación**

El equipo de fabricación debe realizar una serie de pruebas funcionales una vez hayan producido en la fábrica cada elemento perteneciente al sistema.

El resultado de estas pruebas debe quedar reflejado en una Hoja de Registros de Datos.

En el caso del ERTMS N1, se podría obtener una hoja como la mostrada en la Tabla 4.9:

HOJA DE REGISTRO DE DATOS (HRD)			Hoja : 1
ERTMS N1			
COMPROBACIÓN PRUEBA FUNCIONAL			
	Marcar lo que proceda		
	Bien	Mal	N/A
3.- PREPARACION DE DATOS			
3.1 Preparación de datos armario tipo CLC+IR	☐	☐	☑
3.2 Preparación de datos armario tipo CLC	☑	☐	☐
4.- PUESTA EN MARCHA DE LOS CLC's			
4.6.- Comprobar arranque, verificar indicaciones de los SWITCH's	☑	☐	☐
5.- PUESTA EN MARCHA DE LA MOVIOLA			
5.4 Comprobar comunicación de los CLC's y los IR	☑	☐	☐
6.- PUESTA EN MARCHA DE LOS LEU's			
Carga de datos en LEU´s	☑	☐	☐
7.- PUESTA EN MARCHA DEL SIMULADOR DE WESTRACE	☑	☐	☐
7.2.- Lanzado SIMULADOR, displays apagados	☑	☐	☐

Tabla 4.9. Ejemplo de Hoja de Registro de Datos de Fabricación.

- **Hoja de Inspección Final**

La Hoja de Inspección Final es un documento en el que el equipo de fabricación refleja los datos relevantes a nivel de HW de cada componente. En este caso sería su número de serie, el *Rack* al que pertenece, el bastidor en el que se ha instalado, etc.

En la Tabla 4.10 se muestra un ejemplo de HIF para los LEUs:

HOJA INSPECCIÓN FINAL (HIF)			
LEU BP-LMRC			
Nº SERIE	E. MOD.	BASTIDOR	POSICIÓN
E05460947	B	1	LEU 1
E07261221	B	1	LEU 2
E05460948	B	1	LEU 3
E05381270	B	1	LEU 4
E05460942	B	1	LEU 5
E05381279	B	1	LEU 6
E07261855	B	1	LEU 7
E05460905	B	1	LEU 8
E05471202	B	1	LEU 9

Tabla 4.10. Ejemplo de Hoja de Inspección Final.

- **PPIs de fabricación**

Los PPIs (programa de puntos de inspección) son unas hojas con un *checklist* que son necesarias rellenar para cumplir con las especificaciones de calidad impuestas por la empresa suministradora del sistema de señalización.

En el plan de calidad realizado en la primera fase del ciclo de vida, se establecen una serie de *checklist* a rellenar tanto en la fase de producción como en la fase de instalación. Los PPIs de la fase de producción deben ser cumplimentados por el equipo de fabricación, una vez que hayan fabricado el producto.

La Tabla 4.11 muestra un ejemplo de checklist a rellenar en la fase de producción con respecto al sistema ERTMS N1:

PROGRAMA PUNTOS DE INSPECCIÓN				
Referencia / Nº Obra:	**Edición:** 001	**Fecha:**	**Área:** Protección TREN	**Sub Área:** Equipos ERTMS
Proyecto / Obra:			**Enclavamiento, Tren, ...**	
Descripción: ERTMS nivel 1			**Operación:** Pruebas HW Fábrica	

Acciones de verificación	Cuantía	Frecuencia	Comprobación positiva			Verificador (fecha y firma)	Aprobador (fecha y firma)
			SI	NO	N/A		
Inspección visual (montaje componentes, acabado, etc)	100%	Uno por equipo	☐	☐	☐		
Pruebas de cableado y funcionales, cumplimentando HRD.	100%	Uno por equipo	☐	☐	☐		
Identificación PBA's y Módulos cumplimentando HIF.	100%	Uno por equipo	☐	☐	☐		

Tabla 4.11. Ejemplo de PPI de fabricación.

4.7.3 Documentación a generar.

En la fase de fabricación no es necesario que el equipo de seguridad genere ningún documento determinado. Debe revisar los proporcionados por el equipo de fabricación y debe actualizar el *Hazard Log* en caso de que sea necesario.

4.8 Fase VI: Instalación.

Tras haber realizado la fabricación de los subsistemas de manera correcta y tras haberles realizado sus respectivos controles, se procede a la instalación en campo del sistema ERTMS N1 y sus subcomponentes.

4.8.1 Objetivos a alcanzar en esta fase.

Los objetivos de esta fase son:

- Ensamblar e instalar la combinación total de subsistemas y componentes requeridos para formar el sistema completo.

- Iniciar unas pautas de soporte al sistema.

4.8.2 Documentación de entrada.

La documentación de entrada que debe revisar el equipo de seguridad es:

- **PPIs de instalación**

De manera análoga a los PPIs de fabricación, se deben rellenar una serie de *checklist* en campo una vez que ha realizado la instalación de tal manera que se cumplan los requisitos de calidad de la empresa.

- **Registro de instalación de balizas.**

El equipo de instalación debe cumplimentar unas hojas en las que quede reflejado la instalación de cada baliza. En estas hojas se debe identificar cada grupo de balizas y el puesto que ocupa cada baliza dentro de dicho grupo.

- **Hojas de grabación y verificación de balizas**

Las balizas, además de ser instaladas, deben ser grabadas con los telegramas que pueden enviar. Como se ha visto en el segundo capítulo del presente proyecto, hay balizas fijas que envían siempre los mismos mensajes al tren cuando pasa por encima de ellas.

A estas balizas hay que grabarles dichos mensajes. Además de la labor de grabación, se lleva a cabo una segunda comprobación para verificar que los mensajes grabados en dichas balizas son los correctos.

- **Control de versiones instaladas de CLCs y LEUs**

El documento de control de versiones instaladas de CLCs y LEUs recoge las versiones de los LEUs y de los CLCs que se han instalado en la obra. Al igual que con las balizas, primero se hace un registro de la grabación de los LEUs y posteriormente se hace una verificación de la información grabada en los mismos.

En el caso de los LEUs, es necesario anotar la siguiente información:

- ID del LEU
- CLC al que pertenece
- Señal /BG asociado
- *Checksum*
- Versión de datos
- Versión HW del LEU

- **Control de versiones del PCE, PLOs y GR**

El documento de control de versiones del PCE, PLOs y GR recoge todas las versiones de todo el Software instalado en el PCE, los distintos PLO-R y el Gestor ERTMS.

En la Tabla 4.12 se muestra un ejemplo de las versiones SW instaladas de un PCE:

Sistema o módulo	Versión
Sistema Operativo	Windows 7 Proffesional
Java Virtual Machine	1.5.13
Software del PCE	1.0.0.24
Datos	2.0

Tabla 4.12. Ejemplo de control de Versiones del PCE.

- ***Checklist* de instalación del PCE, PLOs y GR**

El checklist de instalación del PCE, PLOs y GR se debe generar debido a que además de tener un registro de versiones instaladas, es necesario realizar una serie de pruebas en campo para los sistemas PCE, PLO-R y el Gestor ERTMS.

- *Checklist* de instalación del PCE y PLO-R:

De manera análoga a las pruebas realizadas en laboratorio para el PCE y los PLO-R, se realizan una serie de pruebas en campo para validar los datos cargados en los equipos.

Las pruebas que se consideran necesarias para la validación de los datos del PCE y de los PLO-R en campo son las siguientes:

- Prueba de verificación de la versión instalada

  El objetivo de la prueba de verificación de la versión instalada es verificar que la versión con la que se están realizando las pruebas es la versión correcta de los datos del PCE.

  La prueba se considerará válida si la versión de datos es la versión correcta de pruebas del PCE.

- Prueba del arranque correcto de PCE con la nueva versión de software.

  El objetivo de la prueba del arranque del PCE es verificar que al instalar el nuevo software en el sistema, este lo acepta y lee correctamente.

  La prueba se considerará correcta si el sistema acepta la nueva versión de software.

- Prueba del arranque correcto de PCE con la nueva versión de datos.

  El objetivo de la prueba es verificar que la nueva versión de datos del PCE se carga correctamente en el sistema y cumple con la funcionalidad especificada.

  La prueba se considerará correcta si el sistema acepta la nueva versión de datos.

- *Checklist* de instalación del GR

En el caso del Gestor ERTMS se rellena una tabla con formato de checklist en la que están ya incluidas una serie de pruebas a realizar tras la instalación. El instalador debe rellenar con un OK/NOK según sea el resultado de la prueba.

La Tabla 4.13 muestra un ejemplo de pruebas a realizar al instalar el Gestor ERTMS:

Nº	Verificación Canal Generador	Comentarios	Estado
1	Comprobar que el PC utilizado cumple los requisitos mínimos del Gestor: • 2 CPUs a 3 Ghz • 2 Discos Duros SCSI de 80 GBytes en RAID 1. • 4 tarjetas ethernet 100/1000 Mbps • 2 GBytes de Memoria RAM ECC • Monitorización de Temperatura • Monitorización de los ventiladores del PC • MTBF de 25000 horas a 25ºC • PC marcado con CE.		
2	Comprobar que el sistema operativo cumple con los siguientes requisitos: • versión estable del kernel 2.4.X • GUI no estará configurado • Servidor SSH activo • GCC 3.x.x instalado		

Tabla 4.13. Ejemplo de Checklist de instalación del GR.

4.8.3 Documentación a generar.

La documentación a generar por parte del equipo de seguridad es la siguiente:

- **Auditoría de despliegue**

La auditoría de despliegue tiene como objetivo comprobar que las actividades de seguridad para la fase de instalación, cumplen los requisitos de seguridad establecidos en el Plan General de Seguridad.

La metodología a seguir es la de recoger evidencias en campo de una muestra escogida al azar de los componentes instalados relacionados con la seguridad. Se utiliza como guía de captura de información, un cuestionario del tipo lista de chequeo en el que se recogen las evidencias que demuestran el cumplimiento de las directrices marcadas en el Plan de Seguridad para cada uno de los componentes suministrados.

Si existen evidencias para todos los campos, el resultado será satisfactorio (OK). Si no existen evidencias debe ser abierta una No-Conformidad (NC).

En la Tabla 4.14 se muestra un ejemplo de lista de chequeo:

LISTA DE CHEQUEO DE LA AUDITORÍA DE SEGURIDAD DEL DESPLIEGUE DE LA APLICACIÓN ESPECÍFICA				
1	**Instalación**	**Sí / No**	**Evidencias**	**Comentarios**
1.1	¿Coincide la versión HW con la recogida en el mapa de equipos instalados?			
1.2	¿Coincide la versión SW con la recogida en el mapa de equipos instalados?			
1.3	Está el componente correctamente identificado en el mapa de equipos instalados			
1.4	¿Existen evidencias de la correcta utilización del Manual de Instalación? ¿Se respetan las condiciones de instalación y ajuste del componente genérico?			
1.5	¿Se he rellenado la hoja de captura de datos correspondiente?			
2	**Validación**			
2.1	¿Existe registro de las pruebas efectuadas sobre el componente en campo?			
2.2	¿Se valida los requisitos funcionales aplicables al componente con esta prueba?			
2.3	¿Se valida los requisitos de seguridad aplicables al componente con esta prueba?			
2.4	¿Es satisfactorio el resultado de la prueba efectuada?			
2.5	¿Son completas las pruebas efectuadas para validar el componente y la integración entre ellos para integrar el subsistema?			

Tabla 4.14. Ejemplo de checklist para Auditoría de Despliegue.

4.9 Fase VII: Validación.

La fase de validación se desarrolla después de que el sistema se haya instalado en campo. Durante esta fase, el equipo de seguridad debe comprobar que se han realizado todas las pruebas necesarias tanto en laboratorio como en campo, y que el resultado de dichas pruebas es el esperado.

4.9.1 Objetivos a alcanzar en esta fase.

El objetivo principal de la fase de validación es:

- Validar la combinación total de subsistemas, componentes y medidas de riesgos externos en cumplimiento de las exigencias RAMS del sistema.

4.9.2 Documentación de entrada.

La documentación de entrada que debe revisar el equipo de seguridad es:

- **Pruebas en vía**

Las pruebas en vía son las pruebas que se realizan en real una vez que se ha instalado ya el sistema. Se utiliza un tren que lleve incorporado una Eurocabina activa de tal manera que se puedan realizar las pruebas necesarias para el sistema ERTMS N1.

Las pruebas en vía se pueden dividir en tres grandes grupos:

- Pruebas de localización de grupos de balizas:

  Las pruebas de localización de grupo de balizas se hacen para verificar que existe coherencia entre la localización programada en los datos ERTMS N1, cargada tanto en los LEUs como en las Eurobalizas, y la localización real de los grupos de balizas.

  La prueba consiste en ir realizando rutas con el tren y en ir marcando los puntos kilométricos en los que la antena del tren lee cada uno de los grupos de balizas. Si estos puntos kilométricos coinciden con los programados, entonces la prueba se da por válida.

  Se recorrerán tantas rutas como sea necesario hasta que queden probados todos los grupos de balizas que se hayan instalado.

- Pruebas de localización de elementos de vía:

  Las pruebas de localización de elementos de vía se realizan con el mismo propósito que las pruebas de localización de balizas. El objetivo de esta prueba es verificar que existe coherencia entre los puntos kilométricos programados en los

datos de ERTMS Nivel 1 relacionados con la ubicación de las señales y las agujas, y la posición real de las mismas.

La prueba consiste en hacer circular un tren por una ruta e ir marcando los puntos kilométricos donde se ubican las señales y las agujas pertenecientes a dicha ruta. Si estos puntos kilométricos coinciden con los programados en los datos ERTMS se considera que la prueba es válida.

Se recorrerán tantas rutas como sea necesario hasta que queden probados todos los grupos de balizas que se hayan instalado.

- Pruebas en vía de funcionalidad:

Las pruebas en vía de funcionalidad se realizan para verificar el correcto comportamiento del sistema para las principales funcionalidades del ERTMS Nivel 1.

Para cada funcionalidad se definen una serie de escenarios que deben ser probados. Dentro de estos escenarios se define el punto de partida de la prueba y el resultado final esperado.

Las funcionalidades que deben ser probadas en vía son las siguientes:

- Entrada en modo *Full supervision*.
- Acortamiento de la autoridad de movimiento.
- Prolongación de la autoridad de movimiento.
- Movimiento de maniobra para Nivel 1 en modo *Staff Responsible*.
- Rebase de señal.
- Transición de modo desde *Full Supervision* hacia Maniobra.
- Transición de modo desde Maniobra hacia *Full Supervision*.
- Recepción del telegrama por defecto.
- *Timers* de sección.

- **Pruebas de interfaz ENCE-ERTMS en vía.**

Las pruebas de interfaz ENCE-ERTMS permiten verificar la correspondencia entre la información procedente del Enclavamiento electrónico y la que recibe el sistema ERTMS.

La información que se intercambian ambos sistemas se puede dividir en dos grupos:

- Indicación de señales
- Posición de los desvíos

Las pruebas a realizar serán las siguientes:

- Se verificará la información de aspecto de las señales.

  Para cada una de las señales que pertenecen a la instalación objeto de las pruebas, se comprobará el intercambio de las variables *Proceed, On sight* y *Shunting* entre el ENCE y el sistema ERTMS.

  Aunque las señales gobernadas por el ENCE podrán presentar el aspecto Proceed para más de una ruta se considerará como prueba válida la verificación de que dicha información se envía para una ruta de cada tipo, no siendo necesario establecer todas las rutas posibles implementadas en el ENCE.

- Se verificará la información de la posición de las agujas.

  Para cada una de las agujas que pertenecen a la instalación objeto de las pruebas, se comprobará el intercambio de las variables Comprobación Derecha (CD) y Comprobación Izquierda (CI) entre el ENCE y el sistema ERTMS Nivel 1.

  No será necesario repetir todos los casos posibles en el que una aguja puede mostrar los aspectos CD y CI. Será suficiente con realizar un único movimiento para cada una de estas indicaciones.

  Cuando el ENCE envía información del estado de un desvío, se considera que tanto el mando como la comprobación del desvío se encuentran en concordancia.

  Se comprobará para cada uno de los desvíos, formen escape o no con otro desvío, que se envía la información de manera independiente y sólo cuando las condiciones anteriormente citadas se cumplen.

4.9.3 Documentación a generar.

La documentación que debe generar el equipo de seguridad en la fase de validación es:

- **Informe de validación**

El informe de validación sirve para justificar la validación de los componentes del subsistema ERTMS Nivel 1 para una aplicación específica determinada. De esta manera, se demuestra que los componentes del sistema ERTMS Nivel 1 cumplen con sus requisitos de seguridad y se han implementado correctamente.

El informe de validación debe incluir:

- Descripción de los equipos implicados.
- Actividades de validación, incluyendo detalles de configuración, métodos de validación y resultados.
- Conclusiones de los resultados de la validación y recomendaciones en caso de ser necesario.

Las actividades de validación se estructuran de la siguiente manera:

- Software de Aplicación de CLCs, LEUs y Balizas (Datos ERTMS N1).

  Para estos datos, el equipo de seguridad realiza las siguientes revisiones:

  - Revisión de los Valores Nacionales.
  - Revisión de las Velocidades de liberación.
  - Revisión de las Velocidades máximas de la línea.
  - Análisis de la introducción de datos (Auscultaciones).
  - Revisión de las pruebas de laboratorio.
  - Revisión de las pruebas de LTV en laboratorio.

- Software de Aplicación de los componentes de los puestos de control ERTMS N1 (PCE, PLO-R y GR).

  El equipo de seguridad revisa las pruebas SW tanto en laboratorio como en campo del puesto central de ERTMS (PCE) y del puesto local de ERTMS (PLO-R).

  Las pruebas del Gestor ERTMS se revisan conjuntamente con las pruebas del PCE y del PLO-R.

- Implementación Física de los componentes.

  La actividad de validación a realizar es dar evidencias de la correcta instalación del sistema ERTMS Nivel 1 para la aplicación específica. De esta manera se deben listar todos los registros de instalación generados durante la fase de instalación.

- Integración de los componentes ERTMS N1.

  La actividad de validación referente a la integración de los componentes ERTMS N1 es comprobar que se han realizado todas las pruebas en vía necesarias y que el resultado de las mismas es el correcto.

Una vez realizadas todas estas actividades de validación, si los resultados han sido satisfactorios, el equipo de seguridad puede concluir que los componentes del sistema ERTMS Nivel 1 suministrados quedan validados.

- **Informe de verificación**

El objetivo del informe de verificación es demostrar que las actividades para cada fase del proyecto se han realizado según lo establecido en el Plan de seguridad y que los objetivos de dicha fase se han cumplido.

A través de la realización de revisiones de diseño durante el desarrollo del proyecto se consigue asegurar que el producto satisface las especificaciones en cuanto a trazabilidad, ciclo de vida, seguridad, etc., y operación en el mínimo coste y en los plazos previstos.

Además las revisiones de Seguridad tendrán en cuenta las siguientes consideraciones:

- La responsabilidad de la gente involucrada es la correcta y cumple con la organización del proyecto.
- El contenido del documento es adecuado y cumple con requisitos y/o objetivos.
- Se comprueba que el grupo de seguridad participa en las revisiones de los documentos de alto nivel, como Especificación de Requisitos y Especificación de pruebas, entre otros.
- Todos los documentos cumplen con los estándares de Calidad y Seguridad y los procedimientos de la empresa suministradora.

Se deben rellenar una serie de fichas de verificación. El campo "resultado" de las fichas de verificación contiene un OK si se cumplen las condiciones mencionadas anteriormente.

Las actividades de verificación de acuerdo con la norma EN 50126 Ref. [1] son:

1. Asegurar que, por cada fase del proyecto, la información usada como entrada para las tareas de cada fase es la adecuada e incluye la información necesaria para completar las tareas de la fase y proporcionar las salidas necesarias para la siguiente fase.
2. Asegurar que los requerimientos de cada fase cubren las salidas de la fase anterior (trazabilidad en las fases del ciclo de vida).
3. Asegurar que por cada fase del proyecto, los requerimientos de la fase han sido satisfechos cumpliendo el objetivo de la fase.
4. Evaluación de la idoneidad de la información y, cuando proceda, de los datos y otras estadísticas utilizadas como información aportada para tareas dentro de esta fase.

5. Confirmar que los métodos, herramientas comerciales y técnicas utilizadas en cada fase son las apropiadas.

6. Evaluación de la competencia de todo el personal que desempeña tareas en al fase.

4.10 Fase VIII: Aceptación.

Una vez que se ha llevado a cabo la instalación en campo de todos los sistemas que componen el ERTMS Nivel 1 y que el equipo de seguridad ha realizado todas las actividades de validación y verificación necesarias, se procede a la aceptación del sistema. Cuando el sistema es aceptado por parte del equipo de seguridad, se considera que esta listo para su puesta en servicio.

4.10.1 Objetivos a alcanzar en esta fase.

El objetivo de esta fase es evaluar el cumplimiento de la combinación total de subsistemas, componentes y medidas de reducción de riesgos externos con las exigencias RAMS para el sistema completo y la aceptación formal del sistema para entrar en servicio.

4.10.2 Documentación de entrada.

En la fase de aceptación, se puede considerar como documentación de entrada toda la documentación que se ha ido generando a lo largo del ciclo de vida. Esto se debe a que todos los informes, pruebas y auditorías elaborados a lo largo de todas las fases desarrolladas con anterioridad, van a ser necesarios para la generación del *Safety Case* del sistema.

4.10.3 Documentación a generar.

- ***Safety Case***

El *Safety Case* o Caso de Seguridad es, junto con el *Hazard Log*, el documento más importante de todo el ciclo de vida del sistema.

En el *Safety Case* se recogen las evidencias del cumplimiento satisfactorio de todas las condiciones de seguridad necesarias para la aceptación de la aplicación de ERTMS N1.

El *Safety Case* sigue la estructura definida en la norma CENELEC 50129 Ref. [2] y debe contener:

- 1ª Parte: Definición.

  En este apartado se define la aplicación y sus interfaces, estableciendo el ámbito de validez del presente Safety Cases

  La aplicación de los componentes ERTMS N1 garantiza la circulación de los trenes en ERTMS N1 cumpliendo su misión: *Ordenar por medio de la señalización la velocidad permitida en cada punto, teniendo en cuenta el*

sentido de circulación, sin que la ruta así señalizada pueda ser invadida simultáneamente por otra circulación.

Para cumplir la misión de ERTMS la aplicación de sus componentes deben garantizar el cumplimiento de las condiciones de aplicación de cada uno de ellos. Las funciones de seguridad de los componentes de ERTMS son las que se han generado en el Análisis Preliminar de Riesgos.

En este apartado se vuelven a incluir dichas funciones de seguridad obtenidas del Análisis Preliminar de Riesgos.

- 2ª Parte: Informe de gestión de calidad.

  En este apartado se detalla cómo el sistema de gestión de la Calidad cumple con lo descrito en el Plan de Calidad desarrollado por la empresa suministradora.

  Para ello se analizan desde el punto de vista de los procesos de calidad, los siguientes apartados:

  - Organización.
  - Planificación y procedimientos de calidad.
  - Especificación de requisitos.
  - Control de diseño.
  - Verificación y revisión del diseño.
  - Ingeniería de aplicación.
  - Fabricación y acopio.
  - Inspección y prueba.
  - Manipulación, almacenamiento y entrega.
  - Identificación de productos y trazabilidad.
  - No conformidades y acciones correctivas.
  - Instalación y puesta en servicio.
  - Operación y mantenimiento.
  - Documentación y registros.
  - Control de cambios.

- Competencia y preparación del personal.
- Auditorías de calidad y seguridad.
- Restirada del servicio.

- 3ª Parte: Informe de gestión de la seguridad.

  En este capítulo se muestran las evidencias necesarias para demostrar que la Seguridad del proyecto ha sido gestionada mediante procedimientos de seguridad efectivos, en concordancia con la gestión de RAMS (Fiabilidad, Disponibilidad, Mantenibilidad, Seguridad) descrita en la norma CENELEC EN-50126 Ref. [1].

  Esta gestión pretende reducir en lo posible la incidencia de errores humanos relacionados con la seguridad durante el ciclo de vida, y por tanto minimizar el riesgo residual de averías sistemáticas.

  En este apartado se deben incluir los elementos del proceso de gestión de seguridad, y proporcionar las evidencias documentales que demuestran la conformidad con todos los elementos del proceso de gestión de seguridad durante el ciclo de vida.

  Para ello, analizan los siguientes elementos:

  - Ciclo de vida del sistema.
  - Organización de seguridad.
  - Plan de seguridad.
  - Hazard Log.
  - Especificación de requisitos de seguridad.
  - Diseño del sistema.
  - Revisiones de seguridad.
  - Verificación y validación de seguridad.
  - Justificación de la seguridad.
  - Aceptación del sistema.
  - Operación y mantenimiento.
  - Retirada del servicio.

- 4ª Parte: Informe de Seguridad Técnica.

  Este apartado contiene las evidencias de seguridad funcional y técnica para la aplicación de los componentes de ERTMS Nivel 1.

  Se deben describir las principales características técnicas utilizadas en el diseño específico y la implantación física de la aplicación de los componentes de ERTMS Nivel 1, justificando su validez para el cumplimiento de los objetivos de seguridad definidos en el plan de seguridad.

  Las secciones que componen en este capítulo son:

  - Garantía de funcionamiento correcto.

    Esta sección se compone de las siguientes subsecciones:

    - Descripción de la arquitectura del subsistema ERTMS Nivel 1.
    - Descripción de los interfaces específicos.
    - Cumplimiento de los requisitos del sistema.
    - Garantía de funcionamiento correcto del SW.
    - Análisis de los datos de aplicación.
    - Correcta implementación física.
    - Puesta en servicio.

  - Análisis del efecto de los fallos.
  - Operación con influencias externas.

    Dentro de estas operaciones hay que analizar:

    - Condiciones del entorno.
    - Condiciones más severas.
    - Protección contra acceso no autorizado.

  - Descripción de las condiciones de aplicación relacionadas con la seguridad.

    Se deben enumerar las siguientes condiciones:

    - Configuración del subsistema ERTMS N1.

- Riesgos exportados ERTMS N1.
- Restricciones de servicio temporales.
- Condiciones de uso.
- Operación y mantenimiento.
- Supervisión de la seguridad operacional.
- Retirada del servicio y eliminación.

- Pruebas de cualificación de seguridad.

- 5ª Parte: Informes de seguridad relacionados.

  En este apartado se incluyen las referencias a cada *Safety Case* e informes de evaluación independiente de cada uno de los componentes que intervienen en el ERTMS Nivel 1. De esta manera se justifica el correcto funcionamiento del HW y SW de cada uno de estos componentes de manera individual.

- 6ª Parte: Conclusiones.

  En el apartado de conclusiones se incluyen las actividades realizadas por parte del equipo de seguridad:

  - Se han realizado las tareas de gestión de la calidad, tal como se establece en el plan de calidad.
  - Se han realizado las tareas de gestión de la seguridad, tal como se establece en el plan de seguridad de la aplicación.
  - Se han identificado las amenazas propias de la aplicación, se han especificado los requisitos necesarios para su mitigación y se ha validado el cumplimiento de los mismos, justificando así la mitigación de las amenazas a niveles de severidad aceptables.
  - Se han realizado las pruebas de laboratorio y vía necesarias para asegurar que los datos de la aplicación son correctos.
  - Se han trasladado al exportador una serie de riesgos exportados, restricciones temporales de servicio y condiciones de uso, derivados de amenazas cuya mitigación queda fuera del alcance del sistema suministrado.

Con estas actividades realizadas, el equipo de seguridad concluye por tanto que la aplicación del sistema ERTMS Nivel 1 para la aplicación específica puede considerarse preparada para su puesta en servicio.

4.11 Fase IX: Operación y Mantenimiento

Tras la puesta en servicio del sistema, es el administrador ferroviario el encargado de la operación y mantenimiento del mismo.

Para ello deberá respetar tanto los manuales de aplicación como los de mantenimiento generados por la empresa suministradora.

El equipo de seguridad ya no tiene ningún papel en esta fase ya que queda fuera de su ámbito de aplicación.

4.11.1 Objetivos a alcanzar en esta fase.

El objetivo de esta fase es operar, mantener y dar soporte a la combinación total de subsistemas, componentes y medidas de reducción de riesgo externo en su cumplimiento con las exigencias RAMS del sistema que se mantiene.

4.11.2 Documentación de entrada.

La empresa suministradora debe generar los manuales de operación y mantenimiento del sistema y debe entregárselos al administrador ferroviario no siendo necesaria la actuación del equipo de seguridad.

4.11.3 Documentación a generar.

Por parte del equipo de seguridad, no es necesario generar ningún documento en esta fase del ciclo de vida.

4.12 Estimación de presupuesto del proyecto

Para poder calcular el coste aproximado de la ingeniería de seguridad descrita en este proyecto, se realiza una estimación tanto de tiempo como de coste para cada una de las actividades de seguridad detalladas en las fases del ciclo de vida.

Se ha estimado que el equipo de seguridad está formado por 2 ingenieros de seguridad y que el coste de cada ingeniero es de 50 €/h.

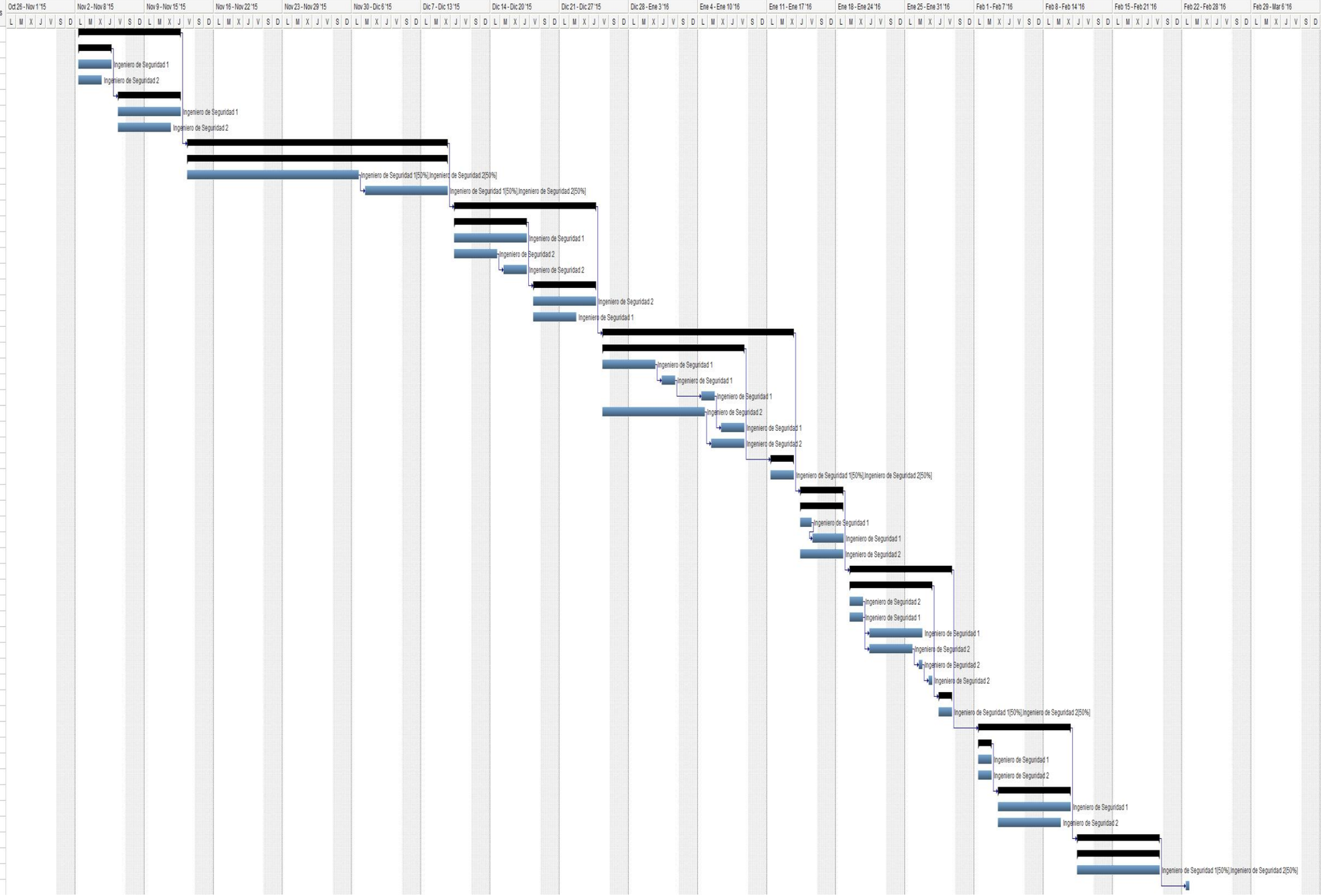
En la Tabla 4.15 se muestra el resumen de la estimación realizada.

FASE	DURACIÓN (Jornadas)	COSTE (Euros)
Fase I: Concepto y Definición	9	6400
Fase II: Análisis de riesgos	19	7600
Fase III: Especificación de requisitos	11	8000
Fase IV: Diseño y desarrollo	14	10000
Fase V: Producción	3	2400
Fase VI: Instalación	9	6000
Fase VII: Validación	8	6000
Fase VIII: Aceptación	7	2800
TOTAL	**80**	**49200**

Tabla 4.15 Resumen de la estimación de la ingeniería de seguridad del proyecto.

La Figura 4.7 muestra el diagrama de Gantt de la ingeniería de seguridad del proyecto para poder cumplir todas las fases del ciclo de vida.

	Nombre	Duración	Coste	Inicio	Fin	Predecesoras
1	**Fase I: Concepto y Definición**	**9d**	**€6400**	**02/11/2015**	**12/11/2015**	
2	**Revisión documentación de entrada**	**4d**	**€2800**	**02/11/2015**	**05/11/2015**	
3	Definición del Sistema	32h	€1600	02/11/2015	05/11/2015	
4	Plan de Calidad	24h	€1200	02/11/2015	04/11/2015	
5	**Generación documentación de Seguridad**	**5d**	**€3600**	**06/11/2015**	**12/11/2015**	**2**
6	Plan de Seguridad	40h	€2000	06/11/2015	12/11/2015	
7	Plan de Validación y Verificación	32h	€1600	06/11/2015	11/11/2015	
8	**Fase II: Análisis de Riesgos**	**19d**	**€7600**	**13/11/2015**	**09/12/2015**	**1**
9	**Generación documentación de Seguridad**	**19d**	**€7600**	**13/11/2015**	**09/12/2015**	
10	Análisis Preliminar de Riesgos	96h	€4800	13/11/2015	30/11/2015	
11	Registro de amenazas	56h	€2800	01/12/2015	09/12/2015	10
12	**Fase III: Especificación de requisitos**	**11d**	**€8000**	**10/12/2015**	**24/12/2015**	**8**
13	**Revisión documentación de entrada**	**6d**	**€4800**	**10/12/2015**	**17/12/2015**	
14	Especificación de requisitos	48h	€2400	10/12/2015	17/12/2015	
15	Especificación de Interfaces	24h	€1200	10/12/2015	14/12/2015	
16	Especificación de Fronteras ETCS	24h	€1200	15/12/2015	17/12/2015	15
17	**Generación documentación de Seguridad**	**5d**	**€3200**	**18/12/2015**	**24/12/2015**	**13**
18	Informe de seguridad de Interfaces	40h	€2000	18/12/2015	24/12/2015	
19	Auditoría de documentación de entrada para el diseño	24h	€1200	18/12/2015	22/12/2015	
20	**Fase IV: Diseño y Desarrollo**	**14d**	**€10000**	**25/12/2015**	**13/01/2016**	**12**
21	**Revisión documentación de entrada**	**11d**	**€8800**	**25/12/2015**	**08/01/2016**	
22	Tira de vía	32h	€1600	25/12/2015	30/12/2015	
23	Informe de auscultación	16h	€800	31/12/2015	01/01/2016	22
24	Informe de gradiente	16h	€800	04/01/2016	05/01/2016	23
25	Protocolo de pruebas en laboratorio de datos	56h	€2800	25/12/2015	04/01/2016	
26	Pruebas en laboratorio de interfaces	24h	€1200	06/01/2016	08/01/2016	24
27	Protocolo de pruebas en laboratorio del sistema de contro	32h	€1600	05/01/2016	08/01/2016	25
28	**Generación documentación de Seguridad**	**3d**	**€1200**	**11/01/2016**	**13/01/2016**	**21**
29	Auditoría de diseño	24h	€1200	11/01/2016	13/01/2016	
30	**Fase V: Producción**	**3d**	**€2400**	**14/01/2016**	**18/01/2016**	**20**
31	**Revisión documentación de entrada**	**3d**	**€2400**	**14/01/2016**	**18/01/2016**	
32	Hoja de registro de datos de fabricación	12h	€600	14/01/2016	15/01/2016	
33	Hoja de inspección final	12h	€600	15/01/2016	18/01/2016	32
34	PPIs de fabricación	24h	€1200	14/01/2016	18/01/2016	
35	**Fase VI: Instalación**	**9d**	**€6000**	**19/01/2016**	**29/01/2016**	**30**
36	**Revisión documentación de entrada**	**7d**	**€5200**	**19/01/2016**	**27/01/2016**	
37	PPIs de instalación	16h	€800	19/01/2016	20/01/2016	
38	Registro de instalación de balizas	16h	€800	19/01/2016	20/01/2016	
39	Hojas de grabación y verificación de balizas	32h	€1600	21/01/2016	26/01/2016	38
40	Control de versiones instaladas de CLCs y LEUs	24h	€1200	21/01/2016	25/01/2016	37
41	Control de versiones del PCE, PLOs y GR	8h	€400	26/01/2016	26/01/2016	40
42	Checklist de instalación del PCE, PLOs y GR	8h	€400	27/01/2016	27/01/2016	41
43	**Generación documentación de Seguridad**	**2d**	**€800**	**28/01/2016**	**29/01/2016**	**36**
44	Auditoría de despliegue	16h	€800	28/01/2016	29/01/2016	
45	**Fase VII: Validación**	**8d**	**€6000**	**01/02/2016**	**10/02/2016**	**35**
46	**Revisión documentación de entrada**	**2d**	**€1600**	**01/02/2016**	**02/02/2016**	
47	Pruebas en vía	16h	€800	01/02/2016	02/02/2016	
48	Pruebas de interfaz ENCE-ERTMS en vía	16h	€800	01/02/2016	02/02/2016	
49	**Generación documentación de Seguridad**	**6d**	**€4400**	**03/02/2016**	**10/02/2016**	**46**
50	Informe de validación	48h	€2400	03/02/2016	10/02/2016	
51	Informe de verificación	40h	€2000	03/02/2016	09/02/2016	
52	**Fase VIII: Aceptación**	**7d**	**€2800**	**11/02/2016**	**19/02/2016**	**45**
53	**Generación documentación de Seguridad**	**7d**	**€2800**	**11/02/2016**	**19/02/2016**	
54	Safety Case	56h	€2800	11/02/2016	19/02/2016	
55	Puesta en Servicio	1d?	€0	22/02/2016	22/02/2016	52



5.Conclusiones y futuros desarrollos

5.1 Conclusiones

El presente proyecto se ha realizado como una aportación a la evolución de la seguridad en el ferrocarril. El tren es uno de los medios de transporte que más han cambiado en los últimos años.

En España, por ejemplo, en algo más de 20 años, se han construido más de 3.100 Km de vías de alta velocidad, consiguiendo vertebrar un país y mejorando la calidad de vida de los viajeros.

Se ha pasado de viajes largos e incómodos, y casi siempre entre grandes ciudades; a trayectos entre ciudades que podían ser más pequeñas, siendo estos viajes más cortos y cómodos, y sobre todo, más seguros.

Y es precisamente en este punto, en la mejora de la seguridad, en el que más se ha centrado el presente proyecto. Esta mejora se concreta en establecer las directrices básicas necesarias para poder instalar un sistema de señalización como es el ERTMS Nivel 1 con todas las garantías de seguridad.

Al comienzo de este proyecto se establecieron tres grandes objetivos a cumplir: Definir los sistemas de señalización y principalmente el ERTMS Nivel 1; aplicar la norma EN-50126 que rige las estrategias a seguir a la hora de realizar una instalación ferroviaria con seguridad; y finalmente establecer el proceso de seguridad paso a paso para llevar a cabo la instalación del sistema.

Complementariamente, y con respecto a los sistemas de señalización ferroviaria, se han definido los elementos que componen un sistema de señalización ferroviaria y se han descrito sistemas de protección de tren, como por ejemplo el ASFA, que no tienen un nivel de seguridad suficiente, ya que depende de las decisiones que tome el maquinista, pudiendo generar situaciones de peligro.

Es por esto que surge la necesidad de implantar sistemas más seguros, que sean capaces de controlar la velocidad del tren en todo momento, que además mejoren la frecuencia de los trenes y que sean sistemas interoperable que permitan el tráfico ferroviario entre

distintos países. Uno de estos sistemas es el ERTMS Nivel 1 y por ello se ha elegido para el desarrollo de este proyecto.

Una vez elegido el sistema de señalización a instalar, es necesario que la empresa suministradora fije una estrategia para desarrollar su producto de manera segura y optimizando en la medida de lo posible los costes. Las grandes empresas de señalización europeas se basan en la norma EN-50126 para definir esta estrategia a través de la ingeniería RAMS.

En este proyecto se han presentado los principios básicos de la norma, definiendo la ingeniería RAMS, los elementos que la componen y los objetivos que se marca. Haciendo especial hincapié en la gestión de riesgos y en el ciclo de vida de necesario cumplimiento del sistema.

Finalmente, se han ido detallando cada una de las fases del ciclo de vida del sistema que afectan a la seguridad del mismo y se han definido las actividades que debe realizar el equipo de seguridad para cada una de ellas, hasta llegar a cumplimentar todo el ciclo de vida permitiendo que se pueda poner en servicio el sistema con las suficientes garantías.

Como conclusión, los objetivos del proyecto marcados se han cumplido, dando suficientes evidencias de la necesidad de la ingeniería de seguridad asociada a la instalación de un sistema de señalización ferroviaria como es el sistema ERTMS Nivel 1, para una mejora integral de la misma.

5.2 Futuros desarrollos

El transporte ferroviario es un medio en constante evolución como se ha comentado en varias ocasiones en este proyecto. Y por lo tanto los sistemas de señalización asociados al ferrocarril también evolucionan a la par.

El propio sistema ERTMS posee dos niveles superiores al Nivel 1 (al cual se ha referido este proyecto). El Nivel 2 y el Nivel 3 del sistema ERTMS suponen una mejora ya que permiten un control continuo de la posición y velocidad del tren, en lugar del control puntual que se obtiene con el Nivel 1, permitiendo una mayor velocidad en los trenes y un aumento en la frecuencia entre ellos. Por otro lado, estos niveles necesitan menos infraestructuras de vía (menos balizas, menos LEUs, e incluso menos señales en el caso del Nivel 3) lo que reduce los costes de implementación en gran medida.

En el caso de la seguridad ferroviaria, también debe evolucionar junto con los sistemas de señalización. En los niveles de ERTMS 2 y 3, los equipos involucrados en la protección del tren no van a ser los mismos (por ejemplo el equipo RBC, que no se utiliza en el Nivel 1), y por tanto las actividades de revisión que deben ser realizadas por el equipo de seguridad van a ser diferentes.

A pesar de eso, los procesos de seguridad no van a variar en gran medida ya que se tendrá que seguir cumpliendo la normativa, de tal forma que se complete el ciclo de vida del sistema, realizando la adecuada gestión de riesgos y generando la documentación de seguridad necesaria para la puesta en servicio.

Glosario

ADIF	Administrador de Infraestructuras Ferroviarias
ASFA	Anuncio de Señales y Frenado Automático
BG	Grupo de balizas
CDS	Concentrador de Detectores de Seguridad
CENELEC	European Committee for Electrotechnical Standardization
CLC	Controlador de LEUs Centralizado
ENCE	Enclavamiento Electrónico
ERTMS	Sistema de gestión de tráfico ferroviario europeo
GR	Gestor ERTMS
JRU	Unidad de Registro Jurídico
LEU	Codificador (Lineside Encoder Unit)
LTV	Limitación Temporal de Velocidad
PCE	Puesto de Central de Operación de ERTMS
PCI	Puesto de Comunicaciones intermedio
PHA	Análisis Preliminar de Amenazas
PLO-R	Puesto Local de Operación de ERTMS
RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio Block Centre
RJU	Registrador jurídico
SAM-R	Sistema de Ayuda a Mantenimiento de ERTMS
SIL	Safety Integrity Level

Bibliografía

Referencia	Título
[1]	EN50126. Aplicaciones Ferroviarias – Especificación y Demostración de la Fiabilidad, la Disponibilidad, la Mantenibilidad y la Seguridad (RAMS).
[2]	EN50129 Aplicaciones Ferroviarias Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización.
[3]	ERTMS System Requirement Specification. Version 2.3.0. Año 2010
[4]	ERTMS Operational Principles and Rules. European Railway Agency. Ed 2. Año 2011
[5]	Requisitos Funcionales y Reglas de Ingeniería ERTMS Nivel 1 y Nivel 2. ADIF. Versión 2.4.6. Año 2012
[6]	Requisitos Funcionales para enclavamientos L.A.V. ADIF. Ed. 02. Año 2009
[7]	Sistema Europeo de Circulación de Trenes (ERTMS/ETCS) ADIF. Año 2005.
[8]	www.aenor.com
[9]	www.ferropedia.es
[10]	www.cenelec.eu